

Guidance

The Institute of Chartered Accountants – NONE

Information Commissioners Office

"When sent by email, consideration should be given to implementing password or encryption controls to documents containing personal and in particular sensitive personal data" (November 2011)

"Appropriate security measures are taken to protect personal data sent by email, in particular sensitive personal data should not be transmitted by email across the internet unless encrypted to current standards" (May 2012)

mercer & hole
chartered accountants

Definition of Sensitive Information

- a) Racial or ethnic origin of data subject
- b) Political opinions
- c) Religious beliefs
- d) Trade Union membership
- e) Physical or mental health condition
- f) Sexual life
- g) Criminal offences

NOT FINANCIAL INFORMATION

mercer & hole
chartered accountants

Survey

Will you send tax returns via emails to clients this year?

Two thirds of the respondents said yes of which –

- 32% applied a password on PDF documents
- 11% encrypted PDF file
- 7% use client portal
- 50% no protection

mercer & hole
chartered accountants

Survey Continued

Will you send accounts via email this year?

78% of respondents said yes of which

- 14% applied a password
- 10% applied encryption
- 10% used portal
- 66% had no protection

mercer & hole
chartered accountants

Survey Continued

Do you use email encryption?

- 32% did not use any encryption
- 36% were considering using email encryption
- 20% had not thought about any protection
- 8% used email encryption
- 4% did not respond

mercer & hole
chartered accountants

Protection used within Mercer & Hole

1. All mobile devices are encrypted including laptops, data sticks, tablets and mobiles
2. Kill packages are available on tablets and mobiles
3. Our standard terms and conditions specifically talk about data protection and electronic communication and draws the clients attention to the fact that emails are not secure

mercer & hole
chartered accountants

Protection used within Mercer & Hole Cont.

4. All hard drives on redundant machinery are "scrubbed" before disposal
5. Sensitive documents can be password Protected using 128 – bit encryption if it is a Microsoft Office file or if Winzip is applied then 256 bit protection is used
6. Our servers use opportunistic TLS (Transport Layer Security) ensuring encryption between servers
7. Mimecast CCM (Close Circuit Messaging)

mercer & hole
chartered accountants

Ep

EMAIL SECURITY RISKS FOR LAW FIRMS



Bernard J. Kubetz, Esq.
Eaton Peabody
80 Exchange Street
P.O. Box 1210
Bangor, ME 04402-1210

Augusta | Bangor | Brunswick | Ellsworth | Portland

eatonpeabody.com

Ep

THE TIMES WE LIVE IN

- Feb. 2014 – *NY Times* reported communications between Mayer Brown, major Chicago law firm, and Indonesian gov't officials were intercepted by Australian intelligence agency



Augusta | Bangor | Brunswick | Ellsworth | Portland

eatonpeabody.com

Ep

THE TIMES WE LIVE IN

(cont'd)

- Last year, several Toronto law firms were targeted by China-based hackers seeking info about a \$40 billion takeover deal




Augusta
Banger
Brunswick
Ellsworth
Portland

eastonpeabody.com

Ep

THE TIMES WE LIVE IN (cont'd)

Has your firm been hacked ?



- You may not know
- 2013 survey by ABA Legal Technology Resource Center
 - 70% of large law firm respondents did not know if breached
 - Risk greater with bring-your-own device policies

Augusta
Banger
Brunswick
Ellsworth
Portland

eastonpeabody.com

Ep

THE TIMES WE LIVE IN

(cont'd)

- Many civil actions are dismissed because Plaintiffs cannot establish injury to a legally protected right or damages when data is breached or lost



Augusta
Banger
Brunswick
Ellsworth
Portland

eastonpeabody.com



THE TIMES WE LIVE IN (cont'd)

- Many courts see loss of data as a hypothetical or future loss not recoverable in the here and now



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



THE TIMES WE LIVE IN (cont'd)

- U.S. Court of Appeals (9th Cir.) held electronic data has value (3/8/2013)
- Landmark decision in *U.S. v. Cotterman* involving border search of registered sex offender



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



THE TIMES WE LIVE IN (cont'd)

- Found uniquely sensitive nature of data from electronic device carries with it significant expectation of privacy



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



THE TIMES WE LIVE IN (cont'd)

U.S. v. Cotterman gives Plaintiffs a legally protected right, an expectation of privacy with constitutional protection



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



WORRISOME LAWS

- **Federal statutes**
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Fair Credit Reporting Act (FCRA)
 - Fair and Accurate Credit Transactions Act (FACTA)
 - Federal Trade Commission Act, § 5



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



WORRISOME LAWS (cont'd)

- **State laws**
 - 2 states, plus Puerto Rico, require notice be given just by virtue of security breach
 - 39 states require a “risk of harm” analysis to determine if notice triggered




Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

WORRISOME LAWS (cont'd)

- **State laws (cont'd)**
 - 20 states require notice to Attorney General or State agency
 - 7 states require notice be given within specific time frame
 - 17 states permit a private c/a
 - 48 (plus 2) provide for encryption "safe harbor"




Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

LAWS OUTSIDE THE U.S.



- Privacy and data protection laws differ significantly
- Personal info may be defined differently

Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

LAWS OUTSIDE THE U.S.
(cont'd)

- In Europe, personal info defined to include business contact info, memberships in trade groups, memberships in political organizations



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

TRANSFER OF PERSONAL INFORMATION ACROSS INTERNATIONAL BORDERS

- Many countries restrict transfer of personal information across borders
- They include Europe, Taiwan, Korea, Japan, Russia, Israel, Switzerland, Australia and Argentina



Augusta | Bangor | Brunswick | Ellsworth | Portland
 eastonpeabody.com

Ep

TRANSFER OF PERSONAL INFORMATION ACROSS INTERNATIONAL BORDERS (cont'd)

- U.S. law firms may be exposed to conflicts between U.S. discovery rules and other countries' data protection laws, potentially subjecting the law firm to sanctions




Augusta | Bangor | Brunswick | Ellsworth | Portland
 eastonpeabody.com


Ep

OBLIGATIONS, PROFESSIONAL CODES OF CONDUCT AND ETHICAL RULES

- Duty of confidentiality is hallmark of attorney-client relationship




Augusta | Bangor | Brunswick | Ellsworth | Portland
 eastonpeabody.com




MODEL RULES OF PROFESSIONAL RESPONSIBILITY

- Rule 1.1**
Attorneys must keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology




Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com




MODEL RULES OF PROFESSIONAL RESPONSIBILITY (cont'd)

- Rule 1.6(c)**
Attorneys shall make reasonable efforts to prevent inadvertent/unauthorized disclosure of or access to info relating to the attorney-client representation



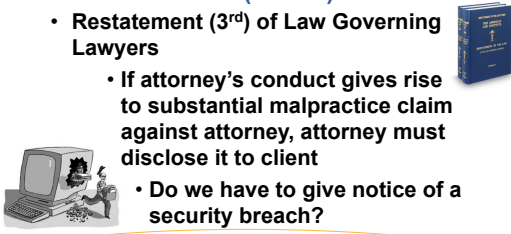
Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



MODEL RULES OF PROFESSIONAL RESPONSIBILITY (cont'd)

- Restatement (3rd) of Law Governing Lawyers**
 - If attorney's conduct gives rise to substantial malpractice claim against attorney, attorney must disclose it to client**
 - Do we have to give notice of a security breach?**



Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

PROPHYLACTIC STEPS

- Audit your firm's security status
 - Who - has access to confidential info
 - What - info your firm has
 - How - received and moves throughout your system
 - Where - info is stored

Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

PROPHYLACTIC STEPS (cont'd)

- Develop an info “retention” policy
- Educate “all” employees
- “FirmLand” Security Officer
- Encrypt confidential data

Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

PROPHYLACTIC STEPS (cont'd)

- Advance to the “rear” regularly / importance of backing up
- “This is a test...”
- Establish and implement email security policy
- Data breach response plan
- Cyber Risk and Data Breach liability coverage


Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com

Ep

DISCLAIMER

The preceding may contain copyrighted material that has been copied under fair use provisions. Any further reproduction or use may not qualify as fair use and may be a violation of copyright law resulting in criminal or civil penalties.



Disclaimer Info

Augusta | Bangor | Brunswick | Ellsworth | Portland

eastonpeabody.com



Traditional & Accepted Communications

Physical paper documents sent via snail mail and fax





Why are we not comfortable sending sensitive data via electronic means, such as emails?

Email security issues



- Sending to unintended recipients
- Emails typically sent without encryption
- Internal vs. external recipients
- No control over an email's lifecycle
- No control over what recipient can do with email

Email security issues cont.



- Limited ability to retract emails
- Limited audit trails and log data of sent emails
- Insufficient abilities to authenticate parties

Specifics to Understand about Email

How does email get from sender to recipient?



VS




Some ways in which an email can be breached


- Sniffers
- Hackers
- Data Miners
- Unintended recipients
- Altered/doctored




Data Breaches are costly



Time Frames




Much cheaper to
avoid than to
experience a breach



Problem – we can't control sent emails

- Could have been delivered to unintended recipients
- What if we realized an error had been made?
- Should recipient have been able to forward or print email?
- What if we wanted to place limits on an email's lifetime?
- How about knowing an email's history?
 - When has it been accessed
 - By who
 - From where



How can your life be made easier?

- You should not be burdened **even more!**
- Solutions should assist us instead of getting in our way of conducting business
 - Automatically provide safeguards
 - Use best security practices
 - Provide us with confidence
 - Give sender control over emails (during composition and after delivery)



Considerations when sending sensitive emails

- Who are you sending the email to?
 - Internal or external communications?
 - Pre-existing or new relationship?
- What should recipient be able to do with the email?
- What restrictions would you like to place on email?
 - Prevent Printing?
 - Prevent Forwarding?
 - For how long should it be accessible?
- Do you want control over email after it's been sent?



Limitations of current email solutions

- Belong to the same group
 - Reasonable for internal communications
 - Requires mutual configuration or pre-communication
- Complicated set-up configurations
 - Requires involvement of IT
 - Intimidating terminology
- Difficulty of use
 - Steep learning curve
 - Use new and unfamiliar email systems
- They don't give you sufficient control



How do I choose a secure email system?

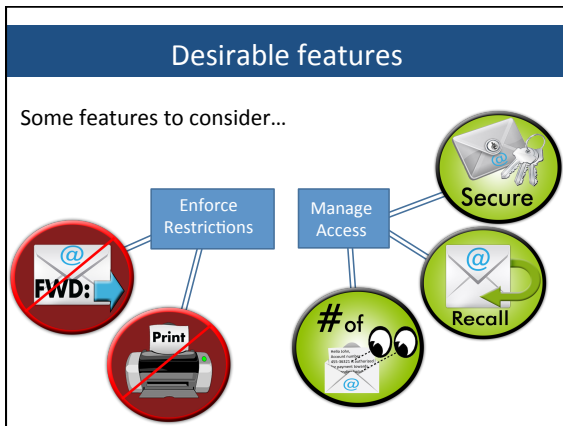


Features & technologies to consider

- Secure internal communications
- Secure external communications
- Sender's controls and restrictions
- Compliant cryptography
- **Simplicity** and usability

How to choose among
available solutions?





Provide Email Audit Trails

John Smith (Accountant) and Dana Jones (Client)

02-Apr-2014 at 3:20pm: John Smith sent original email to Dana Jones
 – Subject: "Your 2014 Tax Return"
 – Location: Miami, FL, USA

02-Apr-2014 at 4:05pm: Dana Jones viewed email from John Smith
 – Location: Chicago, IL, USA

02-Apr-2014 at 4:15pm: Dana Jones replied to John Smith
 – Subject: "Re: Your 2014 Tax Return"
 – Location: Chicago, IL, USA

02-Apr-2014 at 4:48pm: John Smith viewed email from Dana Jones
 – Location: Miami, FL, USA

02-Apr-2014 at 4:48pm: John Smith retracted email
 – Subject: "Your 2014 Tax Return"
 – Location: Miami, FL, USA

Conclusions/Questions

"Business as Usual" may no longer be an option...

Any Questions?

Einar Mykletun, Ph.D.
 Chief Technology Officer
 Identillect Technologies, Inc.
 (888) 781-4080
 einar.mykletun@identillect.com
 Orange County, CA

Defense in depth (best practices)

- Layer 1: Encrypt emails
- Layer 2: Authenticate parties
- Layer 3: Restrict authorized actions
- Layer 4: Controls post sending



Has to be **easy to use!**

Outline

- Email security issues
- Understanding how emails get delivered
- Data breaches are costly
- Problem: we can't control sent emails
- How can your life be made easier?
- Limitations of current solutions
- What to look for when choosing a secure email system?