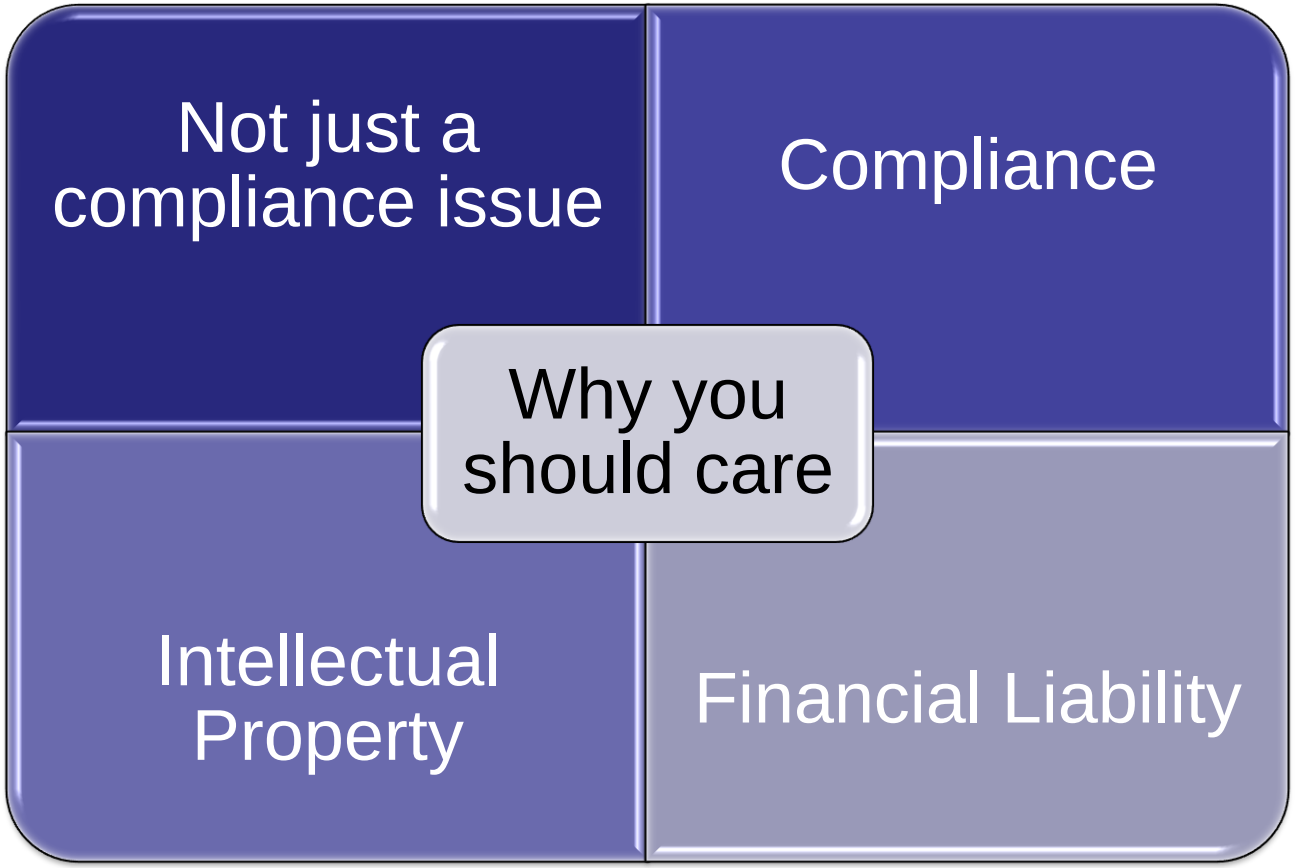
Standards for the Electronic Transfer of Confidential Information

Faculty:

- *Randall J. Rempp, G.D. van Wagenen Financial Services, Inc.*
- *Kimberly Rhodes, Fiberlink Communications Corporation*
- *Jim Brashear, Zix Corporation*
- *Emilo Cividanes, Venable LLP*


Not just a compliance issue
Compliance
Why you should care
Intellectual Property
Financial Liability

Not Just a Compliance Issue....

Intellectual Property

- Protect your Intellectual Property from unintentional disclosure
- Proof of commercially reasonable efforts to protect IP
- Once the cat is out of the bag you can't get it back in

Compliance . . .

- Contractual obligations to protect confidential information and IP
- State requirements to encrypt data in transmission
- State, Federal & International Requirements to use reasonable measures to protect confidential information

Financial Liability

Contractual Liabilities

State & Federal Liabilities

Ponemon Institute Study

- Average Cost in 2010: $7.2 million (each record averaged $214)
  - Includes notification, legal defense, penalties, and lost business
- Malicious & criminal attacks are the most expensive cause and now make up 31% of breaches
- Responses that are too quick can cost 54% more than more methodical responses
- Negligence is still the leading cause: 41%

The Basics: Types of Confidential Information

Types of Confidential Information:

- *Intellectual Property*
- *Trade Secrets: the owner must take reasonable steps to keep it a secret*
- *Financial information*
- *Social security numbers*
- *Customer addresses*
- *Internet browsing habits*
- *Driver's license numbers*

The Basics: Types of Confidential Information

- ***Protected Health Information*** *(reasonable basis to believe it may identify an individual)*
  - ***Individually identifiable health information is:***
    - *Past, present or future physical or mental health records or diagnosis;*
    - *Provision of health care to the individual; or*
    - *Past, present or future payment for the provision of health care*
  - ***Format of the information:***
    - *Transmitted by electronic media,*
    - *Maintained in electronic format, or*
    - *Maintained or transmitted in any other format*

The Basics

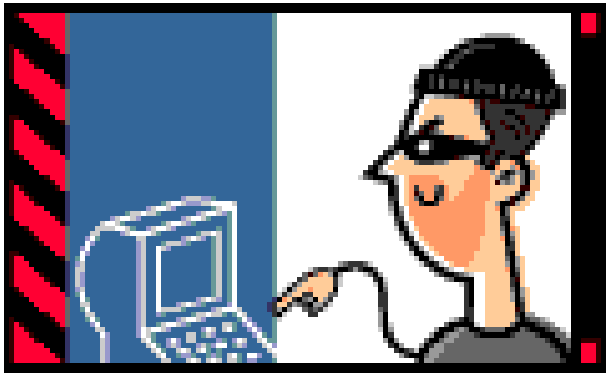
- ***Non-Public Personal Information*** *as defined by Title V of the Gramm-Leach-Bliley Act*
  - *Personally identifiable financial information*
  - *Any list or other grouping derived from personally identifiable information*
  - *Reasonable Basis to Believe it is not NPI:*
    - *Cannot assume information is publicly available*
    - *Must take steps to determine if:*
      - *The information is of the type generally made available to the public*
      - *An individual can direct that it not be made available; and*
      - *If so, whether the particular consumer has directed it not be disclosed*
  - *Examples:*
    - *An individual is a customer of a particular financial institution*
    - *Consumer's name, address, social security number, account number*
    - *Any information provided on an application*
    - *Information obtained from a "cookie"*
    - *Information contained on a consumer report*

Why you need to protect Confidential Information

Contractual Obligations	State Regulations	Federal Regulations
Protection of Intellectual Property & Trade Secrets	International Law	Data Breach Notification
Mitigation of liability in the event of a breach	Protection of Corporate Image	Maintaining Data Integrity

Types of Risks

- System access by computer hackers
- Theft or loss of laptops, thumb drives, smart phones and tablets
- Sharing passwords
- Leaving computer stations unlocked
- Leaving confidential "hard copy" documents, faxes, and mail in unprotected locations
- Holding confidential conversations in non-secure locations
- Error in email recipient
- Theft by an employee
- Third party mishandling of information (vendors)



Federal Regulations Governing Confidential Information

- *Sarbanes-Oxley Act: (see Section 404)*
  - *Requires that a public company must have written policies and procedures that to protect the interests of its stock holders*
  - *If a company maintains client personal information, it must be maintained in a secure manner*
  - *In the event such information is compromised, each affected individual must be informed within a reasonable period of time*
  - *Penalties for Exposure:*
    - *Investigations by the SEC*
    - *Criminal & civil prosecution*
    - *Relinquishing profits realized or loses avoided through the use of the information*
    - *Penalties up to $1 million or 3x the amount of any profits or losses*
    - *Prison terms up to 10 years*
  - *Who is personally liable for compliance violations?*
    - *CEO & CFO must certify all financial statements*
    - *Max penalty for individuals $5 million and $25 for entities*
    - *Up to 20 years in prison*

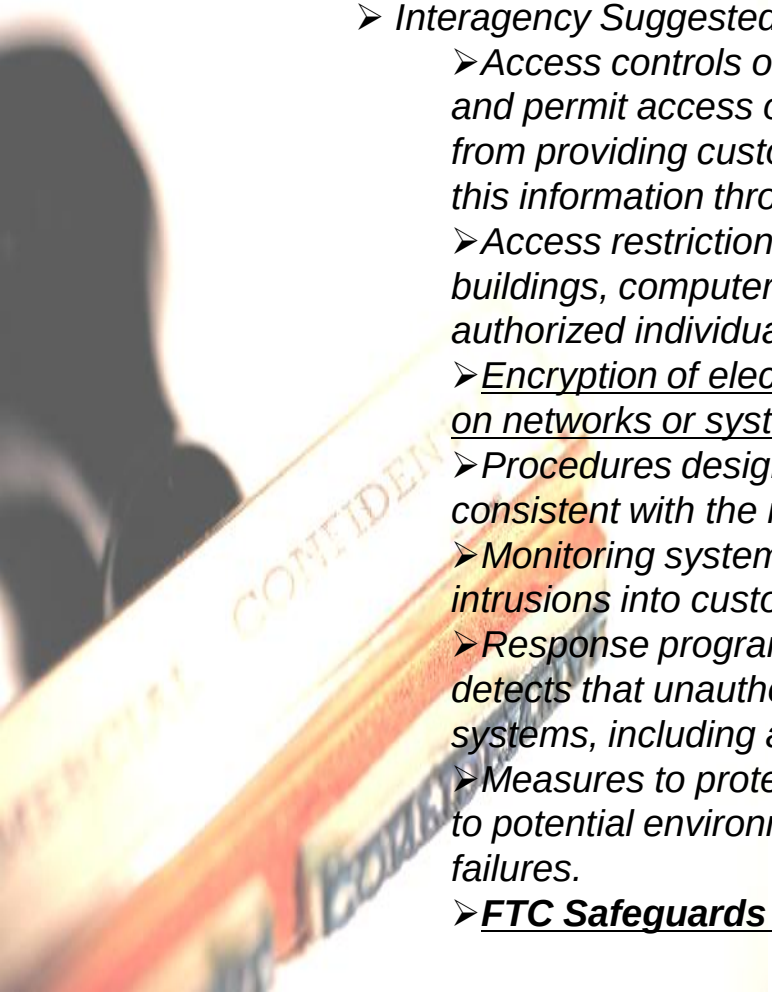
Federal Regulations Governing Confidential Information

- ***Health Information Portability and Accountability Act ("HIPPA"):*** *Privacy Rule (45 CFR Part 160 & Subparts A & E of Part 164)*
  - ***Privacy Policies & Procedures:*** *a covered entity must develop & implement written privacy policies and procedures that are consistent with the Privacy Rule*
  - ***Privacy Personnel:*** *a covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person for receiving complaints and providing information*
  - ***Workforce Training & Management:*** *a covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions*
  - ***Mitigation:*** *a covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information*
  - ***Data Safeguards:*** *a covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information*
  - ***Complaints:*** *procedures for individuals to complain about compliance*
  - ***Document & Record Retention:*** *a covered entity must maintain, until six years after the last effective date, its privacy policies and procedures, privacy practices notices, disposition of complaints and other actions*
  - ***Penalties:***
    - *Civil: $100 per failure to comply with Privacy Rule, not to exceed $25,000 per year*
    - *Criminal Penalties: a person who knowingly obtains or discloses protected health information may be fined up to $50,000 and receive one year of imprisonment. May be increased to $100,000 and 5 years if it involves false pretenses, and $250,000 and 10 years if intended to sell or transfer the information*

Federal Regulations Governing Confidential Information

- *Gramm-Leach-Bliley Act*
  - *Security Guidelines vs. the Privacy Rule*
  - *Sec. 6801:*
    - *Each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and protect the security and confidentiality of the customer's non-public personal information*
    - *Each Agency has establishes appropriate standards relating to administrative, technical and physical safeguards:*
      - *Insure the security and confidentiality of customer records*
      - *Protect against anticipated threats*
      - *Protect against unauthorized access and use of information that could result in substantial harm or inconvenience*
  - *Agencies: Office of the Comptroller of Currency, Board of Governors of the Federal Reserve System, Board of Directors of the Federal Deposit Insurance Corp., Director of the Office of Thrift Supervision, SEC, NCUA, & the FTC*
  - *General Safeguard Guidelines:*
    - *Board of Directors: Oversee a written information security program*
    - *Identifying and Assess Risks*
    - *Manage & Control Risks*
    - *Oversee Service Provider Arrangements*
    - *Adjust the program over time*

Federal Regulations Governing Confidential Information



- *Interagency Suggested Security Guidelines:*
  - *Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;*
  - *Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;*
  - *Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;*
  - *Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program;*
  - *Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;*
  - *Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and*
  - *Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.*
  - ***FTC Safeguards Rule: $11,000 fine per violation per day***

Federal Regulations Governing Confidential Information

- ***Fair & Accurate Credit Transactions Act***
  - *In 2005 FACTA was amended to include a "Disposal Rule" that requires persons and businesses to take appropriate measures in the disposal of confidential information belonging to consumers*
    - *Documents: must be burned, pulverized or shredded so that they are no longer readable*
    - *Electronic files: must be destroyed beyond reconstruction*
- ***GLBA (15 U.S.C. Section 6801 et seq):*** *Requires administrative, technical and physicals safeguards to maintain the security, confidentiality and integrity of consumer information*
- ***Senator Patrick Leahy:*** *has been trying to pass a federal data encryption law since 2005 ("Personal Data Privacy & Security Act")*

State Regulations Governing Confidential Information

- ***Massachusetts:*** *Office of Consumer Affairs & Business Regulation issued a set of regulations effective on January 1, 2009:*
  - *All persons who own, license, store, or maintain "personal information" about a Massachusetts resident must development, implement, maintain and monitor a comprehensive written information security program ("WISP")*
    - *Must be consistent with industry standards*
    - *Contain administrative, technical & physical safeguards to ensure confidentiality*
    - *Consistent with safeguards required for information of similar character as set for in state and federal regulations*
  - *Develop a security policy for employees that takes into account whether and how employees should be allowed to keep, access and transport records*
- ***Nevada:*** *effective October 1, 2008:*
  - *Businesses in Nevada shall not transfer any personal information of a customer through electronic transmission other than facsimile to a person outside of a secure system unless the business uses encryption to ensure the security of the electronic transmission*
- ***Connecticut's*** *Safeguarding and Disposal Rule for Personal Information (effective Oct. 1, 2008)*
  - *Create and display a "privacy protection policy" regarding the collection and use of SSNs*
  - *Safeguard and properly dispose of "personal information"*
  - *An intentional violation of the Privacy Law can result in $500 per violation with a maximum of $500,000 for any "single event"*

State Regulations Governing Confidential Information

- *More than half of all states have enacted laws to limit collection, use and discloser of SSN's*
- *Affirmative obligations to protect personal information*
  - *California, Arkansas, Connecticut, Maryland, Massachusetts, Nevada, North Carolina, Oregon, Rhode Island, Texas & Utah have enacted laws that require the implementation of reasonable security procedures and practices to prevent unauthorized access and use*
- *Oregon's Consumer Identity Theft Protection Act (applies to businesses with over 100 employees): requires the implementation of an information security and disposal program*
- *46 states now have Data Breach Notification Laws*
- *Michigan & Washington are in the process of considering Data Encryption Laws*
- *Texas Identity Theft Enforcement & Protection Act: Grants safe harbor if the data is protected with encryption*

International Regulations Governing Confidential Information

- UK: Data Protection Guidelines as Established by the Information Commissioner's Office
  - The 8th Principle: You must not transfer personal information to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection
  - There are no restrictions on the transfer of personal information to other EEA countries
- Data Protection Directive (95/46/EC) is a European Union directive, that includes:
  - Personal data may only be transferred to third countries if that country provides an adequate level of protection.
  - Directive Article 29 created the Working Party which negotiated the Safe Harbor Principles with the US. Safe Harbor principles:
    - Notice, Choice, Onward Transfer (only to organizations that maintain adequate protection), Security, Data Integrity, Access, and Enforcement of Rules
  - Each EU member is required to provide is own set of data privacy principles and protections under this Directive
  - Generally, EU data privacy laws require employers to institute appropriate technical and organizational measures to protect personal data against accidental or unlawful loss, disclosure or access, especially when that data is being transmitted over a network.

Where is my data???

Wireless Communication

- Data resides in a multitude of locations
  - Within a corporate LAN
  - Smartphones
  - Tablet Computers
  - USB ports
- Can be separated into two major categories
  - Data in Transit and Data at Rest

Securing Wireless Communication

- Data in Transit
  - Data between your company and a third party provider.
  - Needs to be encrypted
    - Specifically, needs to be a vetted encryption algorithm.
    - Should NOT be a “straight,” non-secured protocol.
- Data at rest
  - When information is being processed in a cloud or by third party provider, it is not encrypted.
  - Data lineage should be used.
    - Tells the user where the actual data is.
    - Can be done through mapping application data flows or data path visualization.

Cloud Computing

- What is cloud computing?
  - IT as a service.
  - Data lives with the cloud provider.
- Why would you use a cloud provider?
  - Providers are flexible and changes can be seamless.
  - Pay ONLY for what you use.
- Notable examples include Salesforce and Gmail.

3 Types of Cloud Computing

- Software as a Service(SaaS)
  - Organization outsources the hosting and management of applications to a third party.
  - Typical offering uses a public network in which a SaaS based application is delivered via the internet to the organization's firewall.
- Platform as a Service(PaaS)
  - Cloud vendor offers a development environment to creators of applications.
  - The creators use the platform and offer services through the provider.
- Infrastructure as a Service(IaaS)
  - Vendor provides entire infrastructure for a customer to run his application.
  - Often entails housing dedicated hardware that is purchased or leased for specific application.

Other Examples of Third Party Vendors

- Disaster Recovery Providers
- Data Storage Providers
- Contractors working on premises

Carefully Consider your 3rd Party Provider

- Must be trustworthy and reputable.
  - Providers often have access to customer names, status of prospects, payment information, addresses.
- Liability and Accountability
  - Liability can sometimes be transferred through contractual agreements.
  - Accountability is NOT transferable.
    - In the eyes of the public and the law, the organization that collected information is responsible.

Third Party Provider Security Issues

- Make yourself aware of the provider's protocol for both data in transit and data at rest.
  - Ask provider how they stay current.

- Destruction
  - Data should not be retained for longer than needed to perform task or as required by laws or regulations.
  - When the business relationship ends, data must be completely removed.
    - Make sure the encryption key is destroyed.
    - Make sure files are not just deleted, but overwritten.

Protecting your Client

- Prevent the Initial Breach
  - Carefully vet and analyze third party provider's security practices.
  - Look for certifications (SAS 70), retain audit rights.
  - Make sure the third party provider is up to date and understands the current legislation and regulations.
- Minimize damage in the case of a breach.
  - Breach notification
- Limiting liability in the case of breach.
  - Establish favorable contractual terms
  - Cybersecurity Insurance

Policy to Avoid a Breach

- Use legislation and industry standards to craft data security policy.
  - Stay up-to-date.
  - Go above and beyond the requirements.
    - In the case of a breach, showing commitment to best-practices is key to minimizing liability.
- Education and Training
  - Employees must be aware and knowledgeable of corporate policy.
  - Employees must know significance of breach, and the disastrous potential.
- Consider employing an ethical hacker
  - Someone who spends his or her day attempting to penetrate the system.

Perils of Electronic Data

- **Longevity**
  - Will the format be readable in the future?
- **Zombie Documents**
  - Even when you delete a file, it's not really dead and "gone"
- **Proliferation**
  - Numerous copies on servers, backup tapes, local drives, personal devices
- **Metadata**
  - Document may store information that you may inadvertently disclose in transmission
- **Document security and privacy**
  - Password protection offers limited protection
  - Encryption required for some types of information

Types of "security"

- **Preservation**: Need to retain originals of critical documents for extended periods of time
  - ***Risk***: Destruction, loss
- **Confidentiality**: Need to keep highly sensitive information secret within a limited group of people
  - ***Risk***: Theft, misappropriation
- **Privilege**: Need to keep attorney-client communication and attorney work product protected under applicable law
  - ***Risk***: Discovery, compulsory disclosure
- **Control**: Need to restrict access to and ability to alter critical documents
  - ***Risk***: Unauthorized alteration, material control weakness
- **Privacy:** Need to obscure the relationship between information or activities and the identity of an individual
  - ***Risk***: Identification, identity theft, data breach consequences

Key Data Security Risks

- Loss or theft of device
- Malware
- Hacking
- Phishing
- Social engineering

The Human Factor

The Human Factor

- Users enable security breaches, data theft and corruption:
  - Not backing up data often enough
  - Using same devices for personal and professional data
  - Storing information on unencrypted devices
  - Sending and storing unencrypted data in the Cloud
  - Clicking on unfamiliar links
  - Opening documents from unfamiliar senders
  - Insecure passwords
- Training is essential

Risk mitigation

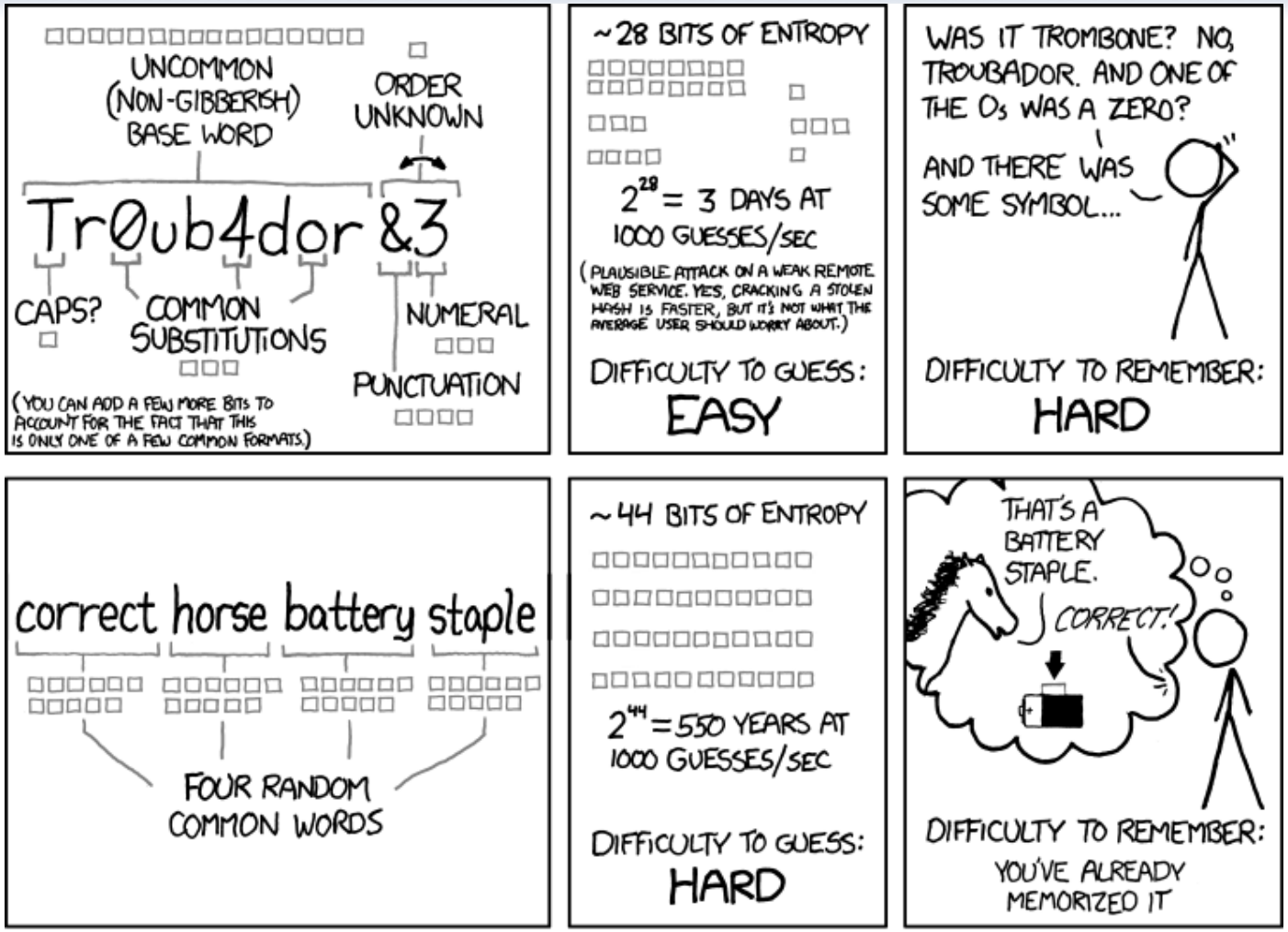
- Common Sense
- Software security updates
- Channel encryption
- Secure portals
- Blockers and trackers
- Metadata strippers
- Automated content encryption

Password Insecurity

- Recent LulzSec hack of 62,000 passwords
- Easily-guessed passwords are common
- ABC123, 123456, QWERTY, Password, etc.
- Same password used for multiple purposes

Secure Passwords

- Don’t use same password multiple places
- Change your passwords regularly
- Strong passwords – Conventional wisdom
  - 12 or more characters
  - No dictionary word
  - Use numbers and special characters
  - Use both upper and lower case letters
- Create password using the first letters in a list or phrase you’ll easily remember

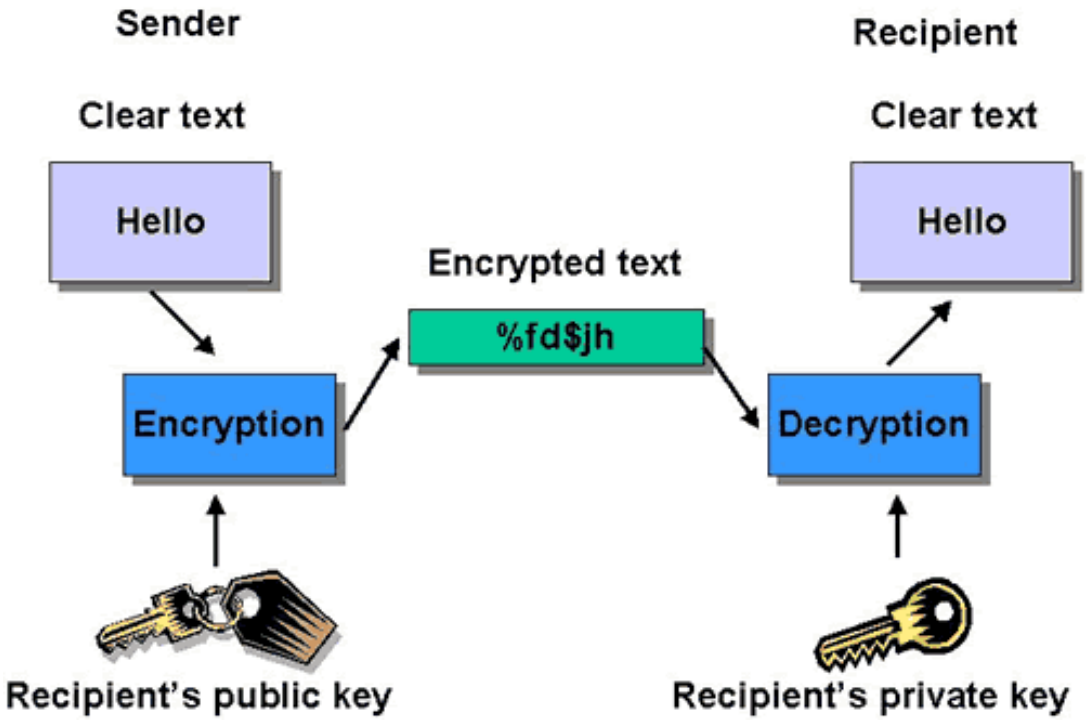

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password Managers

- Consider using a secure, encrypted password manager
  - –Automatically generate secure passwords
  - –Store passwords associated with websites, applications
  - –Automatically complete log-in and forms

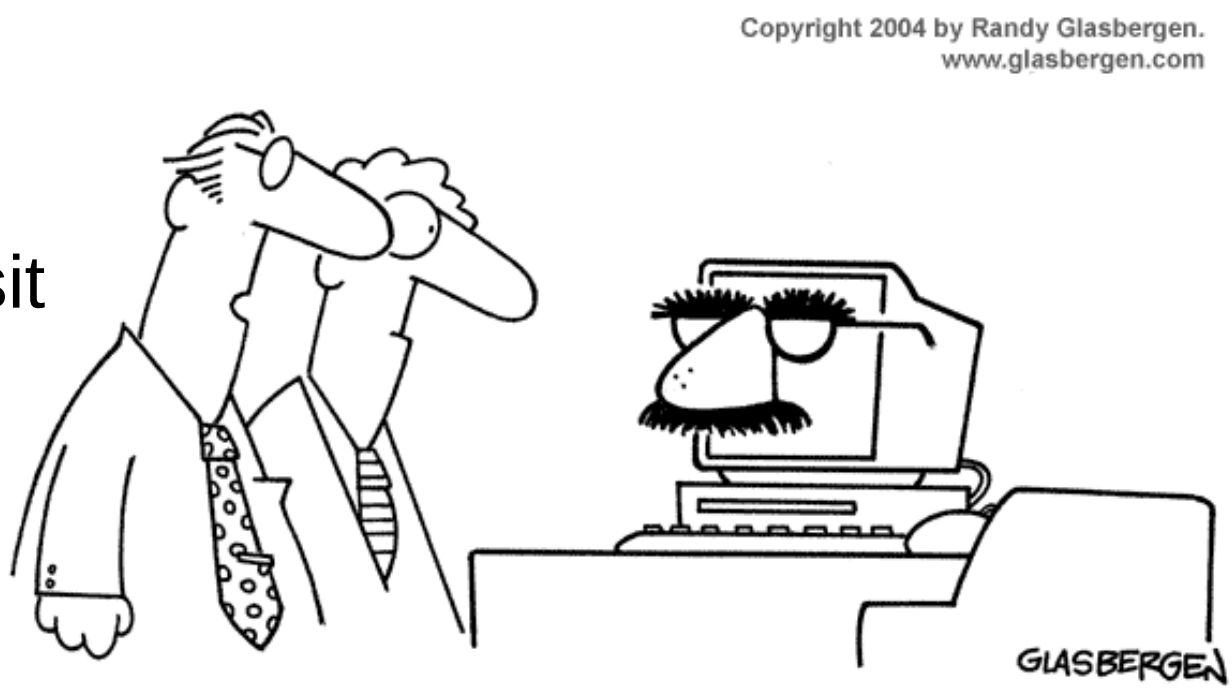
Encryption

- Encryption is a way of concealing data so it remains private between the sender and recipient
- Plain text is converted into cipher text



Encryption applies to

- –Channels
- –Content
- –Data at rest
- –Data in transit



"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

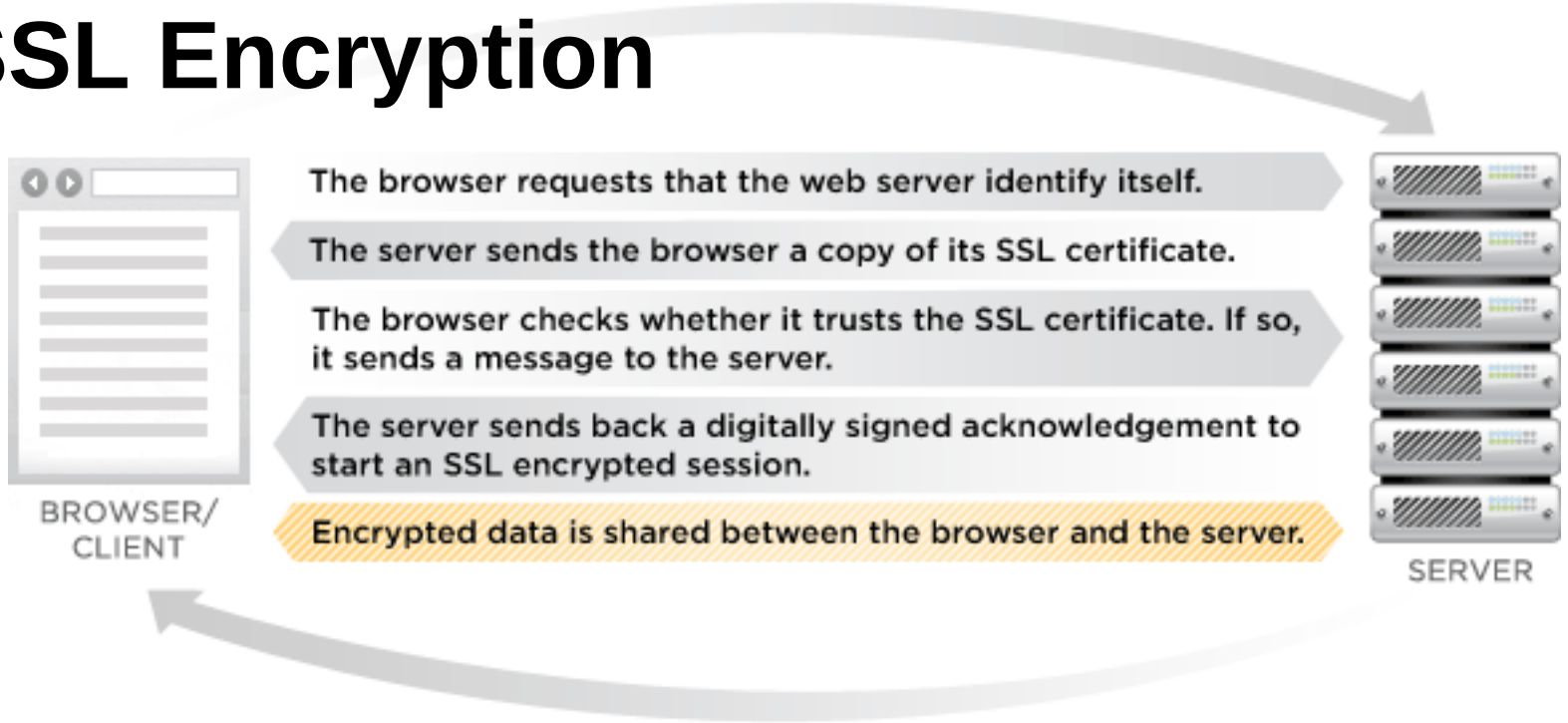
Need to Encrypt Content

- ***Portable device proliferation***
  - *11,000 mobile devices left behind at major US airports in 12 months*
- ***Cloud data insecurity***
  - *Confidential data, including email and attachments, is accessible in the Cloud*
  - *Dropbox inadvertently allowed access to every Dropbox account*
  - *Microsoft BPOS customers could download address book information of other customers*

Need to Encrypt Content

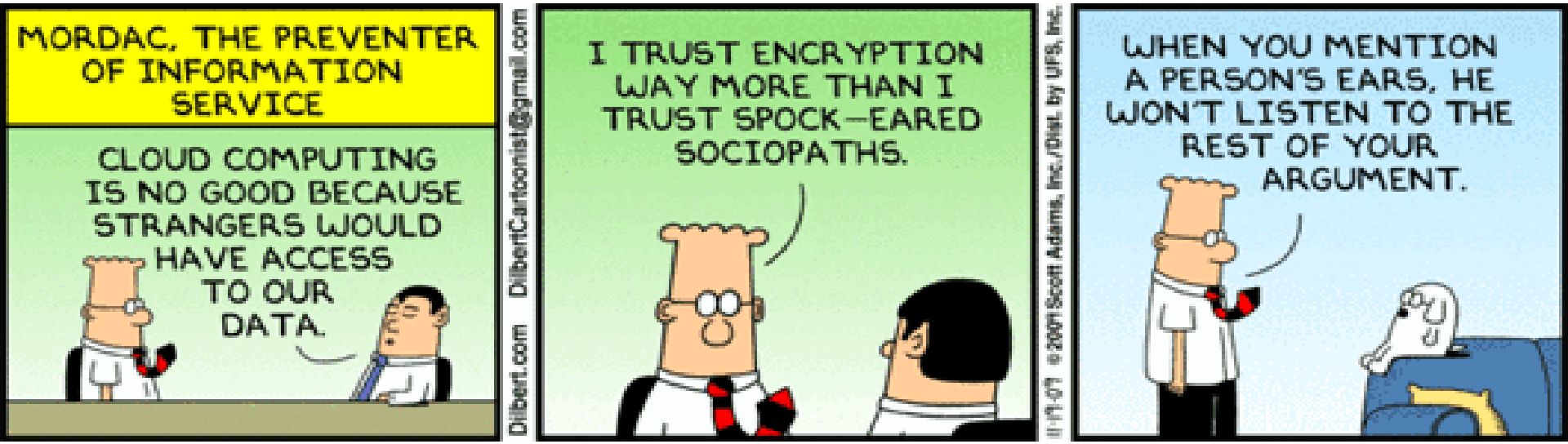
- ***Insecure data transmission***
  - *Open WiFi*
  - *MTM attacks*
  - *SSL certificates untrustworthy*
  - *Internet routing protocols*
    - *2010: 15% of Internet traffic was re-routed through servers belonging to China Telecom (BGP exploit)*

SSL Encryption



- *Creates a HTTPS browser session – the channel is encrypted*
- *Vulnerable to session hijacking and MTM attacks*
- *EFF identified problem with Certificate Authorities improperly issuing SSL certificates*

Cloud Data Storage



Some companies harden enterprise IT systems but send sensitive data outside the enterprise

- Cloud storage, unencrypted devices or unencrypted email
  - Add-ins to automatically encrypt data before it is stored in the cloud
- Consultants, vendors, partners and employees may be the chink in the armor
  - Evidence law firms being targeted by hackers

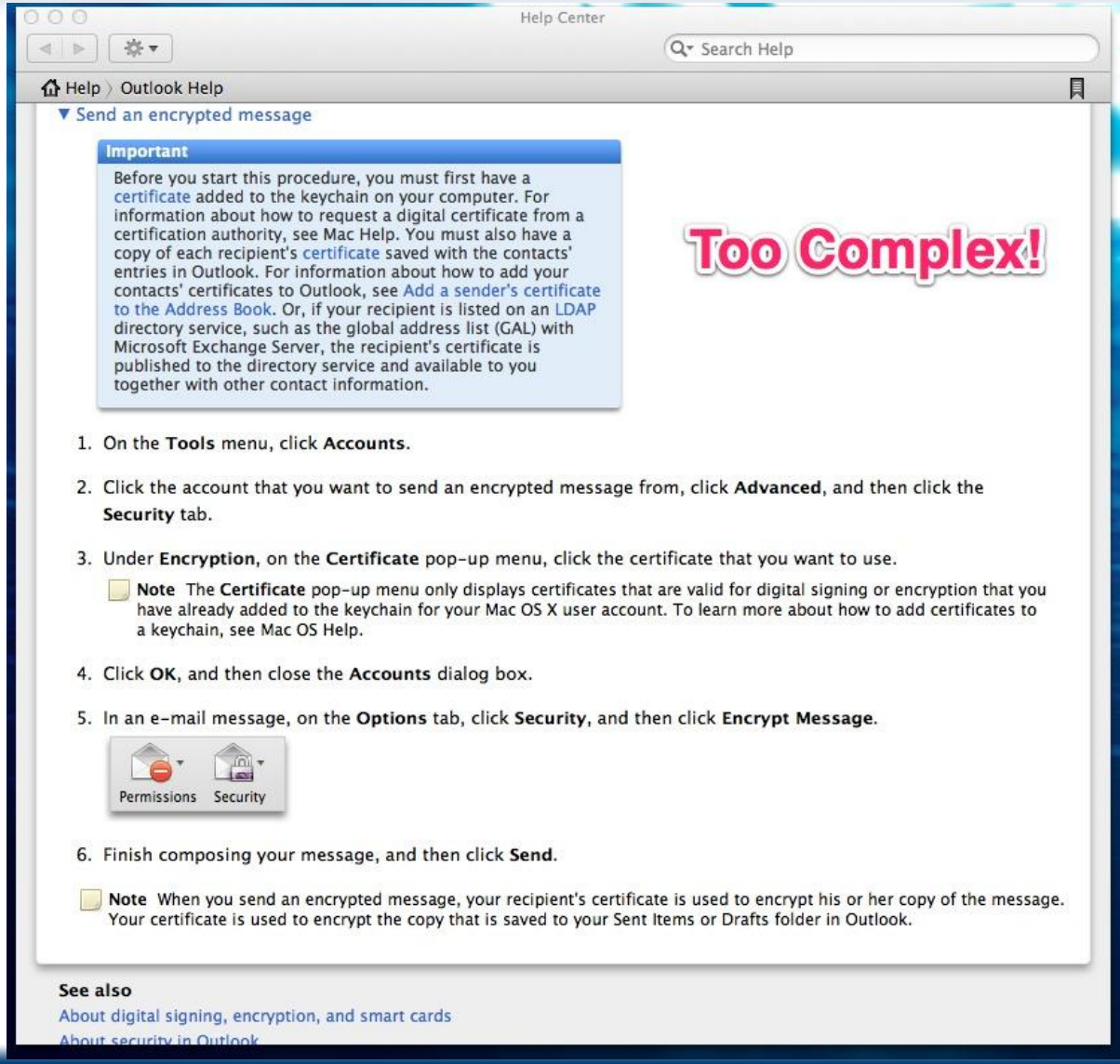
Email and attachments = your confidential data in the Cloud

- *Gartner: "Companies that search for sensitive or private information in email often find it."*

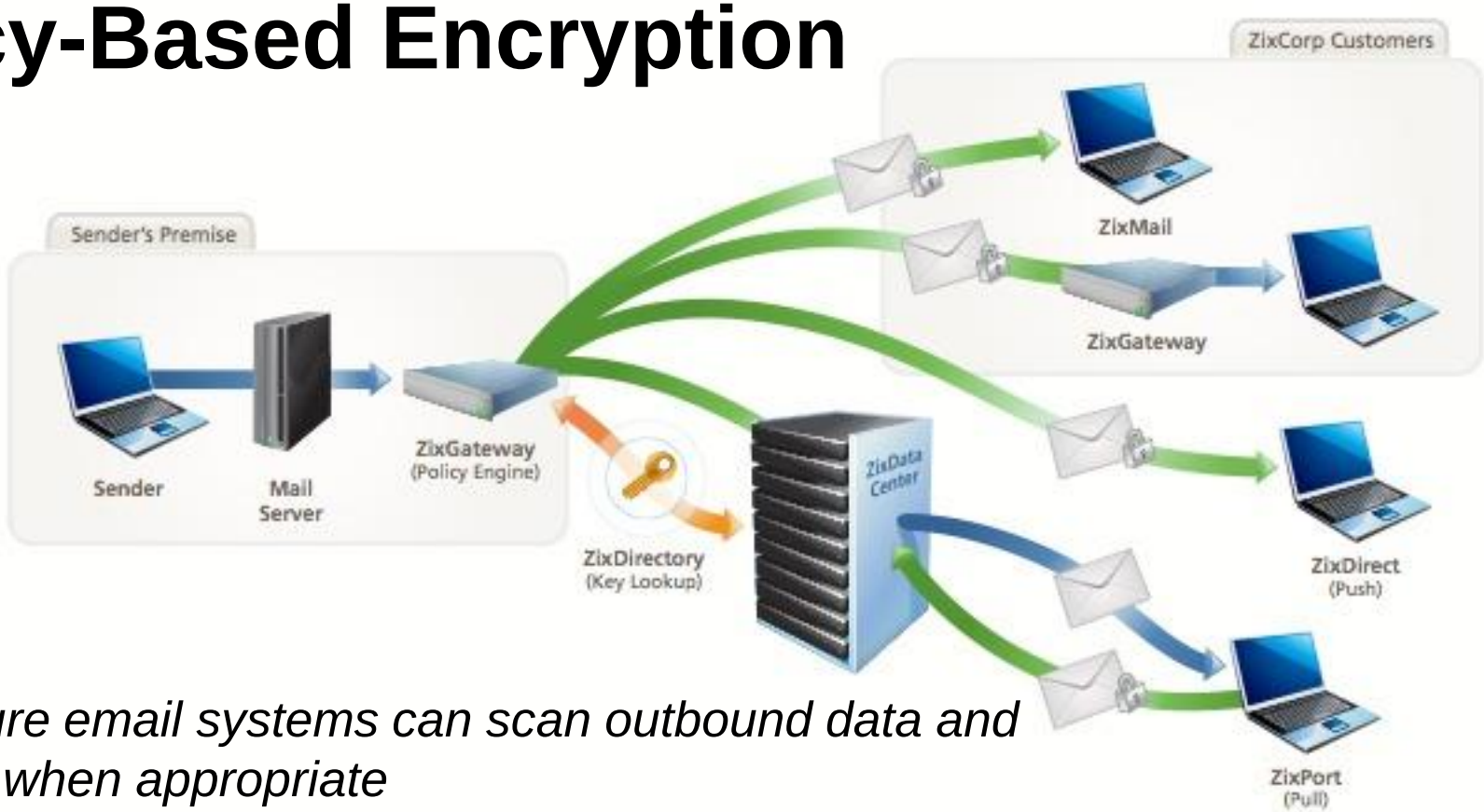
To:

Your competitors and anyone who wants to intercept your email

Why people don't use Outlook's native email encryption



Policy-Based Encryption



- *Best secure email systems can scan outbound data and encrypt it when appropriate*
- *Gartner: "Policy-based encryption is an increasingly important capability and a significant differentiator of leading products."*

Legal Drivers of Encryption

- Data Breach Rules – Encryption Safe Harbors
  - *California: Civil Code 1798.82 "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."*

Legal Drivers of Encryption

- Encryption Mandates
  - ***Nevada****: "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission."*
  - ***Massachusetts****: Personal information about MA residents must be encrypted when stored on portable devices, when transmitted wirelessly or when transmitted on public networks.*
  - ***FINRA Rule 8210****: Requires encryption of all electronic media sent from member organizations to FINRA.*
  - ***HIPAA/HITECH****: An unencrypted email that contains Protected Health Information is sent across the Internet, a violation of HIPAA may have occurred even if the email was not intercepted.*

The Breach: Preparing for and Handling

Shepherding your business through a crisis: breach response

- **Find your incident response plan!**
  - Should set forth protocols for dealing with immediate 72 hours post-discovery of potential breach
  - Notify key members of staff to undertake assigned responsibilities.
    - Legal counsel—both in-house and outside counsel
    - IT staff
    - In-house public relations, media contacts
    - Security staff
    - Compliance staff
    - HR (if breach involved employee data)
    - Relevant business group leaders

Shepherding your business through a crisis: breach response

- **Stress the role of communication and documentation**
  - Move quickly, but key members must remember to document their work and record all steps undertaken
  - Team members must communicate to avoid duplicating effort and to make sure all necessary tasks are completed
- **Evaluating the data: is it compromised or lost/stolen?**
  - The cause of the breach dictates the proper response
  - Compromised data
    - Easier to determine "what" data is at risk and whether data that requires legal notification is in play
    - Points to flaws in network security and more complex steps needed to repair systems down the road
  - Lost/stolen data
    - May not be able to determine "what" data is at risk
    - May require additional physical security or procedures, but network security remains intact

Shepherding your business through a crisis: breach response

- **Lost or Stolen Media**
  - Identify the scope of what is gone—take inventory of missing items
  - Conduct on-site investigation
  - Engage law enforcement, if necessary
  - Locate backups of missing data
- **Compromised Data**
  - Engage help of forensic and IT experts to remove isolate hacking or virus
  - Identify what data was compromised, with special attention to data that might trigger legal breach notification obligations
- **Compromised Data, etc.**
  - Assess scope of hack
  - What data was targeted?
  - What data was removed?
  - What is the risk of harm?
  - Consolidate the compromised data and align with names

Shepherding your business through a crisis: breach response

- Communicate at all stages
- Tailor communications for various audiences
  - Team members
  - Board/CEO, high level executives
  - Regulators
  - Employees
  - Shareholders
  - Customer base
  - Affected individuals

Shepherding your business through a crisis: breach response

- **Determine if obligation to provide notification exists**
- 46 states + DC, PR, and USVI require notification if "personal information" was, or reasonably is, believed to have been acquired by an unauthorized person
  - "Personal information" generally includes an individual's name combined with at least one another "data element"
    - SSN
    - Driver's license number
    - Financial account number in combination with any password that would permit access to a person's account
  - State laws have significant and conflicting variations
  - Arkansas, California, Delaware, and Missouri include medical information
- **Timing of notification**
  - "Majority rule"—in the most expedient time possible, and without unreasonable delay
  - Three states, FL, OH, and WI, impose 45 day requirement
  - May delay notification consistent with law enforcement, except in IL

Shepherding your business through a crisis: breach response

- **Means of notification**
  - U.S. mail
  - Email, if individuals have agreed to email notice
  - Phone, in certain states
  - Substitute notice, if individual notice is too burdensome
    - Test for burden varies
    - Often described as over 500,000 individuals and/or notice costs more than $250,000

- **Contents of notification**
  - Some states dictate mandatory language to be included
  - One example is Maryland, which requires contact information for credit reporting agencies, FTC and state AG, and a statement that the individual can use these resources to learn more about identity theft

Preparation in case of a breach: How to be ready

- **Prepare an incident response plan**
  - To direct a prompt investigation, and the detection and prevention of ongoing activity;
  - To direct the restoration of systems' security and integrity;
  - To address prevention;
  - To provide plan for notification of relevant individuals within the company and their roles;
  - To provide plan for notification of external parties affected by the incident;
  - To provide plan for notification of regulatory agencies and law enforcement, if necessary;
  - To provide plan for prompt disclosure or financial reporting, if required.
- **Contents of the incident response plan**
  - Designated leader(s) for investigation and response
  - Contact information for internal team
  - Contact information for external vendors for security, forensics, etc.
  - Internal reporting system to engage legal, senior management, communications, IT, and other internal personnel
  - Contact information for law enforcement and regulatory and enforcement agencies
  - Steps for investigation of incident and preparation for response

Preparation in case of a breach: How to be ready

- **Who should coordinate the response?**
  - One individual (and backup), typically from legal or the chief privacy officer
  - Liaises between management and response team
  - Coordinates efforts among all groups, coordinates communication, documents the response and handles engaging vendors
- **Who's on your emergency contact list?**
  - Emergency contact list should include the following people:
    - Key people from executive management team
    - Legal, privacy & compliance
    - Security & IT
    - Customer Service
    - HR
    - Communications and Public Relations
  - Designate internal reporting structure

Preparation in case of a breach: How to be ready

- **Law Enforcement contacts**
  - Notify law enforcement if the incident involved suspected illegal activities
  - Depending on size of breach and activities, could notify FBI, Secret Service, or local law enforcement
- **How to investigate and contain the breach**
  - Isolate affected systems, preserving system logs and back-up systems;
  - Make back-up copies of affected data;
  - Retain vendors, such as forensics and systems vendors, to assist with investigation if necessary;
  - Document these steps

Preparation in case of a breach: How to be ready

- **Assessing scope of the response**
  - Assess whether notification to affected individuals is required by law
  - Assess whether notification to insurance carriers, card holder associations, etc., may be required
  - Assess whether to provide affected individuals with identity theft protection services, credit monitoring, etc.
  - Press strategy and press response
  - Government affairs strategy
- **Post-incident debrief**
  - Have a plan in place, post-notification, to review the sequence of events
  - Don't just forget the incident ever happened!
  - Reflect lessons learned by adjusting security and undertaking other necessary steps

Discussion:
How the landscape will continue to change...

Questions & Answers