

W. David Snead, P.C. 

The Third International Conference on Technical and Legal Aspects of the e-Society

CYBERLAWS 2012

Legal Issues Involved in Creating Security Compliance Plans

W. David Snead
Attorney + Counselor
Washington, D.C.

W. David Snead, P.C. 

The Third International Conference on Technical and Legal Aspects of the e-Society


CYBERLAWS 2012


Legal Issues Involved in Creating Security Compliance Plans

W. David Snead
Attorney + Counselor
Washington, D.C.


Roadmap W. David Snead, P.C. 




Roadmap W. David Snead, P.C. 



- ~ What is Security?
- ~ What societal emphases prevail?
- ~ Regulation
- ~ Creating a compliance plan
- ~ Case study
- ~ Toolkit

What is security? W. David Snead, P.C. 

- ~ Is security binary?
- ~ What is a breach?
- ~ Who are the parti
- ~ Who has to be no
- ~ Who are the parti
- ~ Which societal er
- ~ How do we make determining facto
- ~ How do you meas
- ~ What role should
- ~ Are you a special snowflake?





Sophisticated Attacks	Complex Heterogeneous Infrastructure	Information Explosion	Increased Cost of Incidents
-----------------------	--------------------------------------	-----------------------	-----------------------------



By 2011 **1 billion** mobile devices will access the internet

98% of breached data in 2009 came from Apps and Servers

spend **\$6.4 billion** on Cloud in 2014 up from \$3.8 billion in 2010

17% of physical servers virtualized by 2010



600% in 5 years to 988 exabytes in 2010

88% of companies can't answer "what are our information risks today" in less than 2 weeks

Corporate information grows **~66%** every year

600 million email messages are sent a day containing unencrypted confidential data



Value of digital information stolen in 2009 was ~ **\$1 trillion**

Average cost of a data breach in the EU is **€97** per record

total cost of a data breach in the EU is **€2.12 million**

38% view banks less favorably after a data breach

Sophisticated Attackers

News
 Hackers lock Zeus crimeware kit
 Windows-like anti-piracy tech
 Ties do-it-yourself botnet software to a single PC using activation code

photo: Albert Gonzalez
 U.S. Law Enforcement

EMPLOYEE

90% of breaches involved organized crime targeting corporate information

97% of breaches in 2009, compromising 140 million records, used customized malware

48% of breaches involved insiders before malware mutation 15%


What is security? W. David Snead, P.C.

- ~ What is a breach?
- ~ Who are the parties to a breach?
- ~ Who has to be notified?
- ~ Who are the parties to a data transaction?


Which societal emphases prevail? W. David Snead, P.C.

- ~ Stability?
- ~ Confidentiality?
- ~ Law enforcement?
- ~ Compensation / making whole?


"We're from the Neighborhood Watch committee. We've heard you're wearing a fake Rolex."


Which societal emphases prevail? W. David Snead, P.C. 

- ~ Transparency
- ~ Imperfect information
- ~ Competitive pressures
- ~ Lack of definition
- ~ Imperfection in software
- ~ Risk perception

Which societal emphases prevail? W. David Snead, P.C. 

- ~ Social engineering
- ~ Risks perceived incorrectly




Which societal emphases prevail? W. David Snead, P.C. 

- ~ What is the information asset?
- ~ What is the vulnerability?
- ~ Is there a safeguard?
- ~ What is the threat?
- ~ Who/what is the threat agent?

What role should government play? W. David Snead, P.C.


- ~ Mitigation?
- ~ Avoid?
- ~ Transfer?
- ~ Retain?




Regulation W. David Snead, P.C.




Regulation W. David Snead, P.C.



~ Issue Based	~ Sectoral Based
~ Proactive	~ Reactive
~ National implementation	~ Generally state based
	~ Narrowly tailored

Regulation W. David Snead, P.C. 



Legislative and Regulatory Targets

- ~ Breach – both benign and malicious
- ~ Breach notification
- ~ Transfer of risk
- ~ Security policies
- ~ Contracting parties, third parties and vendors

HIPAA

- Specific Safeguards
- Protect against reasonably anticipated uses
- Ensure that workforce complies with rule
- Civil penalties
- Actions by state AG
- HHS investigations

GLB

- Security and confidentiality of customer information
- Protect against anticipated threats or hazards to security and integrity
- Protect against unauthorized access or use.

FCRA

- Identification / Authentication procedures
- Disposal rules
- Procedures to ensure accuracy
- Integrity / accuracy of information sent out
- Attempts to prevent impersonation fraud.

COPPA

- Secure webservers
- Delete personal information after use
- Limit employee access to day
- Provide training
- Screen third parties


FCC

- Protect the confidentiality of CPNI
- Reasonable measures to prevent and discover unauthorized access

FTC

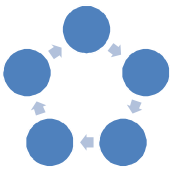
- Unfair or deceptive acts

Regulation W. David Snead, P.C.





- ~ Massachusetts leads the way
- ~ Generally address confidentiality
- ~ Typically only include information tied to numbers
- ~ Beginning to include biometric data
- ~ Nexus requirement – except for Massachusetts
- ~ Exceptions for minor breaches / encrypted data

Regulation W. David Snead, P.C.



- ~ U.S. continues to prefer sectoral regulation
- ~ Breach approached from a confidentiality viewpoint
- ~ Private rights of action disfavored
- ~ FTC likely to have overall responsibility
- ~ Nexus requirement still the norm
- ~ Privacy / security interaction involves identification numbers.

Regulation W. David Snead, P.C. 



- ~ Data governance laws are here to stay
- ~ Expectation that in some format data breach will be extended to cover not just telecoms
- ~ General data breach requirements in some EU Member States already
- ~ Accountability and transparency principles
- ~ Broad scope of definition of personal data
- ~ Cloud and jurisdictional challenges
- ~ The role of controllers and processors


ePrivacy

- Data breach notification
- Addressing lack of harmonization

95/46

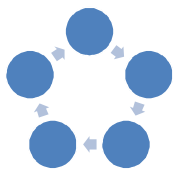
- Breach notification
- Standard privacy notices

Regulation W. David Snead, P.C.



- ~ Only Austria and Germany have breach laws
- ~ Country-by-country data privacy regulations
- ~ Through data retention laws
- ~ No nexus requirement
- ~ Privacy tied to individual information


Regulation W. David Snead, P.C.




- ~ EU continues to prefer industry regulation
- ~ Breach approached from a confidentiality viewpoint
- ~ Private rights of action disfavored
- ~ National laws lag
- ~ Privacy tied to individual data

Creating a compliance plan W. David Snead, P.C.

- Business risks
- Operational risks
- Legal risks
- Regulatory risks

Creating a compliance plan W. David Snead, P.C. 



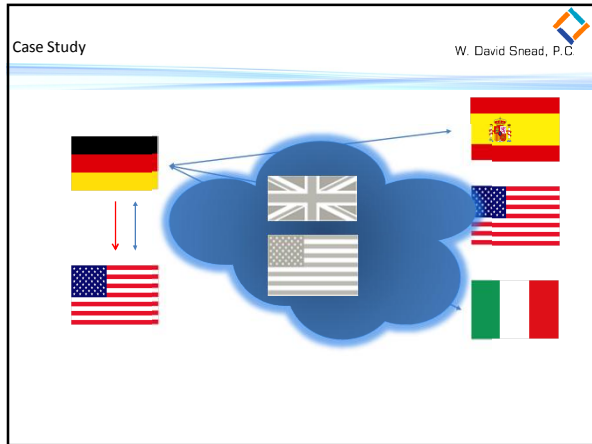
- " Security assessment
- " Legal assessment
- " System and data availability
- " Data retention
- " Social and cultural issues

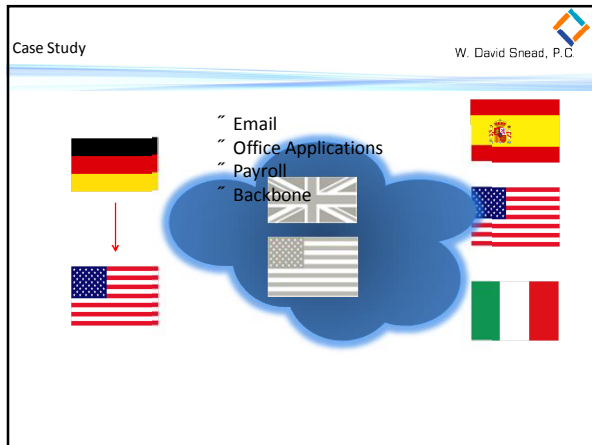
Analyzing the Data Protection/Security Challenges

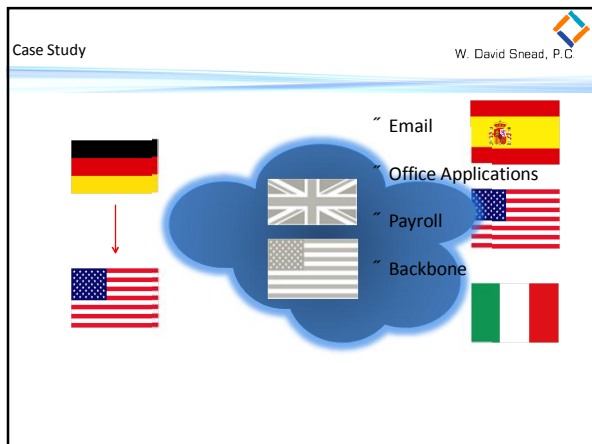
- Develop and Enforce IT Policies
- Protect the Information
- Authenticate Identities
- Manage Systems
- Protect the Infrastructure

This translates to.....


- Develop and Enforce IT Policies *Policy Driven and Risk Based*
- Protect the Information *Information and*
- Authenticate Identities *Identity Centric*
- Manage Systems *Well Managed over a*
- Protect the Infrastructure *Secure Infrastructure*







Creating a compliance plan W. David Snead, P.C.




Business risks ~ Infrastructure
 ~ Support
Operational risks ~ Management
 ~ Delivery
 ~ Pricing

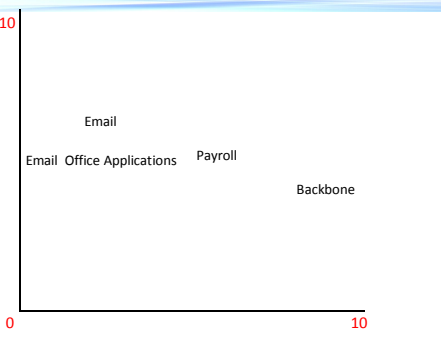
Legal risks

Regulatory risks

Creating a compliance plan W. David Snead, P.C.



Use 10




Email

Email Office Applications Payroll Backbone

0 10

Provider

Creating a compliance plan W. David Snead, P.C.



- Breach definition matches contract
- Internal notifications
- External notifications
- Law enforcement activity
- Investigation
- Secure / mitigate personally identifiable information

Creating a compliance plan W. David Snead, P.C.

- Create methods to address data leakage.
- Require confidentiality agreements
- Secure the data, not the perimeter
- Enforce your policy around the data, not the enterprise or state boundaries.
- Flow down contract terms to vendors
- Do not assume security ends upon termination


Creating a compliance plan W. David Snead, P.C.

- Do you know where sensitive information resides and how to protect it?
- Can you lower costs AND improve your security posture by rationalizing your security
- Can you enforce IT policies and remediate deficiencies?
- Can you control who has access to your information?
- Do you know how the services will be used
- Can you easily manage the lifecycle of your IT assets?
- Have you researched breach notification?
- Have you researched high risk regulatory areas?

Creating a compliance plan W. David Snead, P.C.


Business risks	1. Identify <input checked="" type="checkbox"/> gaps
Operational risks	2. Craft policy
Legal risks	3. Build <input checked="" type="checkbox"/> structure
Regulatory risks	4. Train <input checked="" type="checkbox"/> and communication

Creating a compliance plan W. David Snead, P.C.

 **Security**


- " Define "breach"
- " Determine when a breach happens
- " Assume there will be data breach laws
- " Review any laws that my currently exist
- " Understand who will be responsible for security
- " Create enforceable contract terms
- " Remember post termination issues
- " Understand that you may not be made whole

Creating a compliance plan W. David Snead, P.C.

 **Contract provisions**

- " Breach: benign and malicious.
- " Breach: parties, third parties, subcontractors, vendors
- " Breach laws: Germany, U.K., possibly U.S.
- " Responsibility for security: parties, third parties, subcontractors vendors
- " Post termination issues: data belongs to sol vidro, breach liability extends post termination.
- " Security policy: made part of contract. Revisions subject to sol vidro review. Flow down to subcontractors and vendors

Creating a compliance plan W. David Snead, P.C.


 **Contract provisions**

All data, including, but not limited to, metadata, transactional information, and IP addresses is the sole and exclusive property of Sol Vidro, its affiliates, subsidiaries and assigns. Vendor warrants and represents that this claim of ownership shall be included in all contracts and agreements with third parties who have access to this data. The provisions of this paragraph shall survive termination or expiration of this Agreement. All limitations of liability set out in this agreement shall not apply to a breach of Vendor's obligations set out in this paragraph.

Post termination issues: data belongs to sol vidro, breach liability extends post termination.


Security policy: made part of contract. Revisions subject to sol vidro review. Flow down to subcontractors and vendors

Creating a compliance plan W. David Snead, P.C.

 **Contract provisions**


Vendor has provided Sol Vidro with a copy of its current security policy (Policy) as it applies to the services to be performed by Vendor pursuant to this Agreement. Vendor represents and warrants that this security policy represents best of breed security procedures in its industry. Vendor shall give Sol Vidro no less than sixty days prior written notices of any changes in the Policy that impact the services provided to Sol Vidro. Should Sol Vidro determine that these changes materially impact the security of the services, Sol Vidro will have the right to terminate the Agreement. ~~Security policy made part of contract. Revisions subject to Vendor review. Flow down to sub-factors and vendors its services to another provider.~~

Creating a compliance plan W. David Snead, P.C.


 **Policy provisions**


- ~ Document data to which you have access
- ~ Limit the number of employees who have access to data
- ~ Create and implement access policies
- ~ Create and implement deletion policies
- ~ Flow down contract terms to vendors
- ~ Do not assume security ends upon termination

Creating a compliance plan W. David Snead, P.C.


 **Contract and policy provisions**


- ~ Understand and define law enforcement access
- ~ Don't assume your country's laws will prevail
- ~ Don't let stereotypes interfere with a legal analysis
- ~ Try to create definition

Creating a compliance plan W. David Snead, P.C. 


 **Contract provisions**






Vendor shall provide Sol Vidro with no less than ten days prior written notice of any governmental request for access to the data. For the purposes of this paragraph only, the term "governmental" includes any law enforcement or similar entity. Should Vendor be prohibited by law from providing this notice, Vendor shall strictly limit any disclosure of the data to that which is required by the law and the written document upon which disclosure is based. Under no circumstances shall Vendor provide access without a written request of disclosure which cites the law requiring such disclosure. Vendor shall require this provision, or one similarly protective of Sol Vidro's rights in all its contracts with suppliers or other vendors who provide aspects of the Services.


Creating a compliance plan W. David Snead, P.C. 







 **Policy provisions**


- ~ Require written notice
- ~ Don't assume validity
- ~ Create and implement access policies
- ~ Centralize decision-making
- ~ Include legal advisor

Creating a compliance plan W. David Snead, P.C. 

-  Security
-  Data transfer
-  Disposition of data on termination
-  Change of control
-  Access to data

Toolkit W. David Snead, P.C. 

-  Determine how services will be used
-  Evaluate cloud structure
-  Understand data collection, processing and transfer
-  Security breach notification
-  High risk regulatory areas
-  Disposition of data on termination

Toolkit W. David Snead, P.C. 

W. David Snead
Attorney + Counselor
Tactical Legal Advice for Internet Business

david.snead@dsnead.com
wdsneadpc / Twitter
thewhir.com / Blog
