InfoSec Meets Legal

ISSA Web Conference
February 22, 2011
Start Time: 9 am US Pacific, Noon US Eastern, 5 pm London

Sponsored by:

ISSA®
Information Systems Security Association
Welcome: Conference Moderator

Allan Wall MSc., CISSP, A. Inst. ISP
Independent Consultant
ISSA Web Conference Committee Member
Agenda

• **InfoSec vs Legal**
  • Michael F. Angelo, CRISC - Chief Security Architect, NetIQ Corporation

• **Data Privacy: In the Workplace and Across the Border**
  • Bill Connolly - Managing Director, Stroz Friedberg

• **Business Records to ESI to Digital Evidence**
  • Hoyt L. Kesterson II - Senior Consultant, Terra Verde Services

• Joint Speaker Question & Answer
• Closing Remarks
InfoSec vs Legal

Michael F. Angelo, CRISC
Chief Security Architect
NetIQ Corporation
Disclaimer

• I am not a lawyer

• This session is aimed at raising awareness, and concern...

• In considering each example, we assume similar issues to the previous example, but do not explicitly call them out.
Agenda

• The Race
• General Laws as an Issue
• Consumerization
• Clouds
• And Mandatory Certifications
The Race

Corporate Problem
• Better ROI
• Work Faster

Technology
• Cloud Computing
• Consumerization

Corporate Adoption
• Cloud
• Consumerization

Criminal Abuse
• IP Theft
• DoS

Response 1
• InfoSec Professionals

Response 2
• Legislative Activity
Oooppss…

- In protecting our systems we may unwittingly / unknowingly violate laws OR
- Laws may be created that make what we are doing illegal.
Legislation: Last Months Presentation

• Mr. Joseph Tasker
  – If Legislation Enacted, How Might that Affect What You Do?
  – More than 20 Cyber Security Bills in Congress in 2010
  – Bipartisan Sponsors, both R’s and D’s
  – Joe.taskerjr@gmail.com
A Common Event

You believe someone (hacker or employee) is trying to steal corporate secrets.

- You monitor all electronic communications. (packets, email, keystrokes).
A Common Issue

• Laws:
  – Electronic Communications Privacy Act (ECPA) (18 USC. 2510)
  – Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)
  – Stored Communications Act (SCA)

• Guidance:
  – http://csrc.nist.gov/publications/nistbul/csI93-03.txt
More Common Examples

You are looking into network anomalies
  – You start looking at log files, then analyze individual machines, and finally disassemble some programs that you think may be an issue.

• Does your analysis constitute reverse engineering?
  – Digital Millennium Copyright Act (DMCA)
More Common Issues

You are served with a subpoena that requires you to comply with the rules for eDiscovery

• Does eDiscovery constitute forensics?

• Do the tools that gather materials for eDiscovery constitute forensics tools?

• The marketing literature says the tool is a forensic tool!!
  – Forensic laws
    • GA, TX, MI, SC, etc
This Weeks Issue

The use of personal equipment in your infrastructure has been allowed.

- You need to examine an employees personal machine (notebook) being used for corporate work.
- eDiscovery?

• Potential Issue(s):
  - Employee PII might be exposed
  - Employee separation & residual data.
Laws

• Need to:
  – Define acceptable use
  – Set expectations for privacy

• Btw.
  – What if you don’t find what you are looking for, but find evidence of another crime?

• Remember Employee with Laptop?
  – What if they are running a bit torrent and sharing movies from your network…
  – S3804 - Copyright Act
Cost Reductions

You have decided to deploy Biometrics to reduce the cost of passwords

• Laws:
  – governing exposure of biometric database
  – governing use of biometrics or biometric data
  – governing sale of biometric data
  – governing transfer of biometric data
Cost Reductions

• Cloud Computing

• Cloud Location
  – Transfer of PII across States and Countries
  – Transfer of Technology
  – Do you know?

• State / Local laws mandating PII protections

• Federal Laws - technology might be ‘exported’

• What if you are using Biometrics for Access to the Cloud?
What About Exports?

Export Laws cover:

• Forensics – that can handle encryption
  – SSL Audit
  – Crypt Breaker's Workbench

• Evaluated Operating Systems
  – => EAL6
New Legislation

• Proposed Mandatory InfoSec Certifications
  – Make it illegal to perform InfoSec functions if not certified
  – Irish - Private Security Services Bill, 2001
  – CyberSecurity Act of 2009 (SB 773) Rockefeller–Snow Bill

• Good News?
  – Not well thought out.
  – No scheme to define certification
Laws / Mandates / Directives and Stuff

If InfoSec is not up to snuff…

• S 3480 – Protecting Cyberspace as a National Asset
  – Isolate non compliant agencies
  – Limitations on liability if compliant
  – What is a Critical Infrastructure Component?
Summary

• Laws and Certifications work best when their target is static and understood or evolving in a known manner.

• The internet continues to experience revolutionary changes in technology and use and so issues that will arise.

• Security Professionals need to make sure they are not painted into a corner, and can continue to protect the assets they are entrusted with.

• Security Professionals MUST work with legislators and governments to educate them, else stupid things can happen.
Conclusion

“there is nothing worse, than a well enforced bad rule.”

Contact Information:

eMail: angelom@netiq.com

Question and Answer

Michael F. Angelo
angelom@netiq.com
Data Privacy: In the Workplace and Across the Border

Bill Connolly
Managing Director
Stroz Friedberg
Employer’s Right to Monitor

• NIST/DOJ Guidance 1993
• NJ Appeals Court


Facts:
– Company sued for failing to investigate employee’s distribution of child pornography
– Company was aware that employee was accessing pornography but did nothing
– Company’s computer security director acknowledged ability to monitor employee

Ruling:
– Company owed a duty of care to the child pornography victim;
– Company had a duty to further investigate employee’s activities;
– Company could have lawfully monitored employee’s computer activity.
Workplace Privacy

• NJ Supreme Court


Facts:
– Employee files sexual harassment claim
– Company forensically harvests web mail from firm computer
– Webmail contains communications with employee’s attorney

Ruling:
– Employee had a reasonable expectation of privacy in personal, password-protected, web-based e-mail;
– Attorney-client privilege overrides written company policy;
– Rule of Profession Conduct violated.
Workplace Privacy

• U.S. Supreme Court


Facts:
– Supervisor allows personal texts on city pagers if overage paid
– City conducts investigation into overage charges
– Officer “sexting” messages discovered to wife and girlfriend

Ruling:
– Officer had privacy interest in texts on city pager;
– Informal statement over-rode formal policy;
– Government search was reasonable
  – Related to work assessment of provider’s text limit
  – Limited to transcripts for 2 months of work-day texts.
Data Protection

U.S. v. EU
Data Protection

EU Data Protection Directive

Article 1 – Object of the Directive

“In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”
EU Data Protection

• **Personal Data** - any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

• Could be email address, ethnicity, tax information

• Not necessarily unique identifying information

• Blocking Statutes re: U.S. discovery
PII in the U.S.

Typically includes a name in conjunction with:

- Social Security Number
- Bank Account Numbers
- Credit Card Numbers
- Dates of Birth
- License Numbers
- Mother’s Maiden Name
- Other Unique Identifying Information
EU data Protection

• Beware of penalties

• Processing” includes collection, organization, storing, retrieving, holding, using, consulting, disclosure by transmitting, copying, making available

• “Onward Transfer” prohibited to non-EU countries unless country ensures adequate protection, unless exception applies (NOTE: U.S. protection inadequate)
  • Transfer permitted when legally required for the purpose of litigation abroad
  • However, wholesale transfer of information may not be considered necessary
Data Protection

E.U.
Each country in the E.U. has its own rules implementing the Directive; Rules vary widely

U.S.
Patchwork of state statutes
Contact Information

Bill Connolly, Managing Director

Phone: 617-848-5661
Email: wconnolly@strozfriedberg.com
Question and Answer

Bill Connolly
wconnolly@strozfriedberg.com
Business Records to ESI to Digital Evidence

the importance of data integrity

Hoyt L Kesterson II
Terra Verde Services
Hello, I’m Hoyt L Kesterson II and…

I AM NOT A LAWYER
The nature of a Writing has changed
The fundamental change in writing has changed assumptions about authenticity

- Old paradigm of *original* — a physical artifact
- Old paradigm of *inspection* of the object — the eye and the hand
- Now
  - digital information objects are pure information
  - digital information objects are *untestable* through inspection
  - there is no meaning to the concept of *original*
- Some believe that one can treat ESI as if it were paper.
But it ain’t paper

• When investigating the authenticity of a physical document, one can look at
  – pen strokes, e.g. weight, speed, vector
  – the integrity of the binding of a ledger
  – composition of physical media

• Digital data can be so ephemeral, so malleable.

• Saving the data and associated information for proof of an action, e.g. a contractual commitment, can be quite daunting.

• Effort should be proportionate to need.
Here’s my evidence

How does one know that the evidence has

– not been completely fabricated?
– not been modified since it was written?
– accurate times and dates
The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created.”
The evidence produced for court

- Will likely be digital, Electronically Stored Information
- Much current discussion on admissibility, i.e. the authenticity of ESI
  - That’s important
  - But let’s not forget…
- Accuracy…Reliability
  - Influences how the evidence will be weighed
  - It’s what juries consider
When a record is created

• If necessary, one will identify its…
  – Creators if it is a *statement* by them
  – Signers if it is, for example, an *agreement* among them

• If necessary, one will state when the record was created

• One must protect it from change and…

• One must protect it from destruction

• One must protect the integrity of the record
  – Including the identity of its creators and signers
  – Including the date and time it was created
Integrity—what is it?

• We are interested in the second and third meanings
• It’s *complete* and it’s *unimpaired*
Integrity—in the beginning

• There was noise
• Engineers tried to put information in the noise
• But noise kept creeping back into information
• Then there was Shannon; he said…
• You can’t keep error (née noise) out
• You must detect it and correct it
• Thus parity bits, CRC, and more
• They detect accidents of nature…
• …but not purposeful manipulation
Integrity—how do we achieve it?

- Store the record in a secure location
  - But what if it must be accessed?
- Make multiple copies
  - Store one with a trusted third party, or
  - Store many copies everywhere, e.g. print in a newspaper
- Apply cryptographic techniques
  - A modification would be tantamount to destruction
    - One must still protect the record to prevent modification
  - These techniques don’t prevent modification—they only prevent undetectable modification
  - Encrypting the document won’t do if it must remain readable.
  - One must create a unique and compact stand-in
Hash functions

• Hash function is one-way.
  – The message cannot be derived from the hash
    • but one could create a set of hashes of all possible values.
  – It’s computationally infeasible to construct two messages to produce the same hash.
  – It’s computationally infeasible to construct a message to produce a given hash.

• Secure Hash Algorithm (SHA-1) is recommended.
  – 160 bit result
    – A weakness has been discovered.

• SHA-2 variants are SHA-224, -256, -384, & -512.

• SHA-3 is expected to be standardized by the end of 2012,
Protect the hash

• If the hash value is not protected, someone could
  – modify a document and compute a new hash value
  – replace the previous hash value with the newly computed value.

• One must protect the hash value
  – by storing it with a trusted third party such as Surety; or
  – distributing multiple copies; or

• Encrypt the hash.
  – If done with an asymmetric key, one has a digital signature.

• A time stamping service can produce a hash that protects the integrity of the document and fixes that value to a specific date and time.
Recording “when”

May require use of a trusted appliance

or

a trusted authority
Time is important…
…without it everything would happen at once.

- Typically one shouldn’t trust a computer’s clock.
- Use trusted time-stamping systems (external provider or in-house).
- Risk should determine the granularity of the timestamp.
- Choose the method that
  — provides the granularity needed;
  — provides a suitable method for subsequent verification;
  — provides the communication model needed, e.g. stay within the enterprise.
Signed, sealed, & unprotected

- Cryptography doesn’t protect a document from change.
  It only prevents undetectable change

- A cryptographically-protected record that is modified or destroyed isn’t good evidence.

- Defense can be multiple copies (e.g. stored at a secured third-party facility), robust authorization and access controls, and/or solid manual controls.

- Long-term storage requires re-sealing with stronger mechanisms
De l'intégrité, encore de l'intégrité, toujours de l'intégrité

• As Danton almost said, it’s always about integrity

• Since ESI can be easily fabricated and modified, one must be able to prove that after the creation of ESI, that the integrity of the ESI has been maintained throughout its storage or use.

• Appropriate deployment varies—small or large organization, public or private.

• Invest in technology proportionate to the business risk. going to jail may be a possible risk to consider.

Choose wisely
Questions?

Hoyt L Kesterson II
Terra Verde Services
hoyt.kesterson@terraverdeservices
Question and Answer

Hoyt L. Kesterson II
hoyt.kesterson@terraverdeservices
Joint Speaker Question & Answer

- Michael F. Angelo
  Chief Security Architect, NetIQ

- Bill Connolly
  Managing Director, Stroz Friedberg

- Hoyt L. Kesterson II
  Senior Consultant, Terra Verde Services
Closing Remarks

Thank you to our Sponsor

STROZ FRIEDBERG

Thank you to Citrix for donating this Webcast service

GoToMeeting™

Online Meetings Made Easy
CPE Credit

• Within 24 hours of the conclusion of this webcast, you will receive a link to a post Web Conference quiz.

• After the successful completion of the quiz you will be given an opportunity to PRINT a certificate of attendance to use for the submission of CPE credits.

To begin the post event quiz now, simply go to: