U.S National Security, Individual and Corporate Information Security, and Information Security Providers

Bryan Cunningham & Forrest Morgan

Morgan & Cunningham LLC

bc@morgancunningham.net

forrest@morgancunningham.net

WARNING: This Briefing ***Is Not Legal Advice***

- Provides an overview of policy and legal issues important to information security professionals
- We *cannot* provide legal advice unless in a retained, legal relationship with specific clients
- You ***cannot rely on these suggestions*** as legal advice
- Following suggestions in this briefing *does not create* any legal defense
- Information security professionals are *strongly urged* to retain qualified and experienced legal counsel

“We Have a Situation”

Cures for White House Insomnia

- Terror Group or Rogue State Uses Hijacked U.S.Computers to Attack the United States

or

- Terror Group or Rogue State Uses Hijacked U.S. Computer to Attack Another Nation *From the United States*

Either Way, We're At War

US Response

- Presidential authorities
- United States Policy:
  - *When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies.*

    -- National Strategy to Secure Cyberspace

US Response (cont.)

"Distinguishing between malicious activity originating from criminals, nation state actors, and terrorists in real time is difficult."

-- *National Strategy to Secure Cyberspace*

A National Strategy

National Cybersecurity Strategy

- Recognizes that healthy functioning of cyberspace is “essential to our economy and our national security.”
- States *all* US critical infrastructure relies on vulnerable information technology
- Rejects (for now) model of gov’t. control of cyberspace
- States that all that own/control cyberspace are responsible for securing it

From National Cybersecurity Strategy

"All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace."

Is this "duty" now U.S. Government policy?

Example: Slammer Sapphire

- Though only attacked one company software for servers, also affected 911 systems, ATMs, airline reservation systems
- Canada *had to cancel an online election*
- Fact that [the worm] wasn't attached to a more destructive payload "leads me to think that it may have been a ***test***."

  --Richard Clarke *as quoted on pbs.org*

Example: Zombies

- Hijacking of business, educational, personal computers for:
- Malicious, criminal, terrorist purposes
- Difficulty of detecting "zombie status" *without intruding on computers used*

Zombies in Action
Operation Casper - January 2005

- Attack - UK: Used compromised computers (“zombies”) to flood Web sites w/useless traffic.
- Objective: To extort a "significant quantity of money" from victims in return for stopping
- Such attacks typically involve hundreds of compromised computers; great increase in past year

Have Your Systems Been "Zombied?" Will They?

- 30000 "zombie networks" in 2004; each with "thousands of bots"

  -- *Richard Clarke, as quoted on www.itfacts.biz*

- Just because you haven't seen it, doesn't mean it's not happening

Ripped From the Headlines

- ChoicePoint: Identity Information Stolen-145,000
- Apparently *Not* Hacking - This Time
- Example of *policy* and *social engineering* flaws being *as dangerous as technical*
- Regulation possible; ***Litigation Already Filed***

Ripped From the Headlines

LexisNexis

- Original estimate = 32,000
- Now at least 10 times that (310,000)
- Words You Never Want to Say:
- ***"I believe there may have been a security breach in LexisNexis prior to 2003 that involved personal data and we did not make notice."***
  - Kurt Sanford, LexisNexis' president and chief executive for U.S. corporate and federal markets, to a US Senate hearing, April 2005

Ripped From the Headlines

Reported May 2005:

- Outside firm "lost" Time Warner **Information on 600,000 current, former workers**
- **Back-up tapes lost during transport for storage**
- U.S. Secret Service investigating

Ripped From the Headlines

April 2005: Wachovia, Bank of America, Commerce Bank

- Account info on 500,000 customers sold
- Conspiracy included employees who sold for $10 per account
- Info bought and used by collection agencies and *lawyers*
- No technical breaches involved at all
- Illustrates importance of *policies* (background checks, etc.)

Ripped From the Headlines

- ***Citigroup***
  - Records on 3.9 million customers “lost” by UPS
  - Data not encrypted
  - Social Security numbers and payment history of U.S. customers
- Illustrates need for contracts/control over info in 3rd party hands
- ***MasterCard***

Ripped From the Headlines

- ***New Details on Cisco-Related Hack***
  - Hacking theft of Cisco router programming instructions
  - For computers that “control flow of Internet”
- Info used to compromise “thousands” of computers, including
- US military, NASA, and research labs

Key Lessons from Cisco Hack

- Was true “hack,” not physical theft or phony customer
- Shows again even sophisticated government, corporate systems vulnerable
- Took *months* to unravel and stop plot
- Swedish teenager responsible
- Launched from University Servers
- University of Minnesota used as “staging base” for “hundreds of Internet attacks”

Bulls-eye on Higher Education

- Universities are preferred targets
  - Highly networked
  - Lots of computing power concentrated
  - Culture of openness
  - Reluctance of government to intrude
  - Historically weak security (generally)
  - Relatively easy “social engineering”
- **No coincidence 1998 “Solar Sunrise” intrusions into Defense Dept. “originated” at Harvard**

Ripped From the Headlines

- University of Kansas
  - Hacked 5 times; foreign student records stolen
- Cal State-Chico
  - 59,000 personal records possibly accessed
- Northwestern
  - Info on 21,000 students, faculty, grads
- UC/Berkeley
  - Laptop w/100,000 names, SSNs stolen
- UC Davis
  - 1100 names, SSNs

Ripped From the Headlines

- ***Carnegie-Mellon April 2005***
  - At least 5,000 students, employees, and graduates
  - Social Security Numbers and other personal info
  - “Hacked”
- “*No clear idea”* how long systems had been vulnerable
- Canegie-Mellon runs U.S. CERT Program

Some Potential Sources of Liability

Federal Statutes & Regulations

- HIPAA
- Gramm-Leach-Bliley
- FERPA (Family Educational Rights & Privacy Act), TEACH Act

Some Potential Sources of Liability

- State Law
  - Deceptive trade practices & other statutes
  - Common law tort liability
  - Unauthorized Access (***you*** *should care)*
- Consent Decrees
  - Microsoft & Ziff Davis last *20 years*
- New Federal Regulation ?

Potential Sources of Liability (cont.)

- Contractual obligations
- Statements on company's website
- Victims lawsuits
- Employee lawsuits
- Shareholder lawsuits
- Individual Officer & Director Liability

Risk of Officer/Director Liability

Sarbanes-Oxley:

- Requires senior management to perform annual assessment of internal controls over financial reporting
- Indirectly requires management to certify data accuracy
- Regulators believe securing data necessary to ensure accuracy and reliability

Global Issues: European Union Privacy Directive

- From 3/31/04: Requires companies to *guarantee the security* of networks and services they provide (information services *and* telecom)
- Extraterritorial jurisdiction
  - Providers within the EU
  - Where one end of communication is in the EU
- Penalties and reach

Other Reasons For Your Customers to Care

- Gov't will regulate if industry doesn't solve
- Negative public image of corporations that don't do all that was reasonable
- *Positive* public image of those that do
- Do well by doing good
- *Your* company can *set* the standard

There’s The Risk

What Now?

Preparation, Not Panic

- No Deer in Headlights
- To Start, You Have to Start
- **Outside, Third-Party Assessment Crucial,** *but*
- Get the Right Advice
- Pick Your Battles

Holistic/& Dynamic Approach Required

- Viable Security Policy = **Both** Technical/ Physical **and** Broader Policy/Compliance
- One without the other = liability risk
- Security Assessments & Adjustments **MUST Be Dynamic and Ongoing**
  - HIPAA/GLB Standards Being Exported
  - Consent decrees/Cyber Security Strategy
  - “Standard of Care” Being Established

Security Cannot Be Static

- "Securing cyberspace is an ongoing process, as new technologies appear and new vulnerabilities are identified."

- Offense always more nimble than defense:
  - Maginot line
  - Iraqi trenches in First Gulf War

Law of Information Security Also Evolving

- HIPAA/GLB Standards Being Exported
- Consent decrees
- “Standard of Care” Being Established
- Reasonable *Under the Circumstances*
  - “Circumstances” will keep changing

Which Better Protects *Your* Secrets (and those of your customer)?

Standard of Care

- Regulations and Consent Decree Standards
- Reasonable Predictor of What Congress/Regulators May Expect in Future
- Also of What Prosecutors and Juries May Conclude Was Reasonable
- External, independent standards such as those of the National Security Agency = Good start

Sources of Emerging Standard of Care

- Common Law
- Statutes (HIPAA, GLB) and Related Regulations
- Consent Decrees
  - Microsoft
  - Ziff Davis Media
- Uniform Commercial Code requires “reasonable security” w/re fund transfers

Common Law Negligence

- ***"Reasonability" =***
- Probability of specific damage occurring
- Severity of damage if it does occur
- Identification of risk mitigation measures
- Cost of implementing such measures
- Balance
- Nothing is bulletproof *but*
- Post-hoc question will be: What was *reasonable* ***under the circumstances***?

Process Plus Specifics

- Comprehensive plan requires individualized business assessment
- Recommend against “security in a box”
- Emerging Standard of Care Requires:
  - Key *Process* Elements; **and**
  - Specific Types of “Reasonable” Security Measures
- No single “checklist” will do

Key Process Elements

1. **Documented *Assessment* of Key *Assets***
   -- Identify "crown jewels" & secure first
2. **Matrix *Threats* Against Identified Assets**
   - **"Reasonably anticipated" Internal & External**
3. **Comprehensive *Risk Management Program***
   - **Technical**
   - **Physical**
   - **Process**
   - **Personnel/Social Engineering (*ER '97)***

Key Process Elements (cont.)

Risk Management Program Take Reasonable Measures to:

- Keep information resources *available*
- Control *access* to information and networks
- Keep personal/sensitive info *confidential*
- Evaluate, monitor, preserve *accuracy* of info
- Prevent *unauthorized alteration* of info

Key Process Elements (cont.)

4. "Step Back" Assessment
   - Everything *surrounding* info-security, e.g.,
     - Personnel policies
     - Confidentiality/non-disclosure agreements
     - Agreements with third parties
     - Legal/compliance
5. Individual *Accountability* for Security
   - Board Routinely Involved
   - Officer/Director Liability (GLB Section 404)

Key Process Elements (cont.)

6. W*ritten Documentation* and Distribution of Security Plan & Policies
7. I*mplementation*, *Training*, and Employee *Accountability* (including in evaluations)
8. Ongoing **External** *Auditing* and *Testing*
9. Ongoing *Modification of Processes & Procedures*

Current Key Specific Types of Security Practices

- Technical Security
- Procedural Security
- Physical Security
- Related Process & Compliance Measures
- Independent Assessment & Testing

Selected Examples of Security Measures Required in Regs/Decrees

- “Independent” Network Monitoring
- Intrusion Detection
- Facility, Device, Network Access Controls
- Technical Anti-Intrusion Measures
- Employee Control Measures
- System Modification Procedures

Examples of Required Security Measures (cont.)

- Data Integrity & Disposal
- Audit Trails
- Backup/Contingency Plans
- Plans for Response to Attacks/Accidents
- Ongoing Assessment and Adjustment
- Neutral 3rd Party Audits

Complete Solution Should Include:

- **Network Assessment and Technical Security Solutions**
- **Physical Security Solutions**
- **Network Monitoring & Intrusion Detection**
- **Policy, Legal, Compliance Solutions**
- **Independent, Outside Evaluation**
- **Incident Response & Mitigation Plans**
- **Post-Incident Communication Plans**
- **Dealing with Law Enforcement, Homeland Security, & Intelligence Agencies**

A Shortcut Not to Take

- **"I only want a penetration test"**
  - **Your customer *Will* fail**
- **That failure will be documented with no way to protect it in litigation**
- **Even if the vulnerability the testers exploited is fixed, customer likely *won't find all the others, but will* have demonstrated awareness of risks, but only took one step**
- **With no protection, *you're a witness***

Why Have a Law Firm Involved (for customers' sake)?

- **Reduces litigation risk**
- **Attorney-Client Privilege for assessments**
- **Ensure security, personnel and related practices comply with applicable laws and regulations**
- **Advice, and influence on legislative/regulatory developments**
- **Guidance on meeting appropriate "Standard of Care"**
- **Dynamic external audits**
- **Crisis management (communications, law enforcement, etc.)**
- **Litigation support**

TOP TEN Reasons to Have a Law Firm Involved (for ***Information Security Consultants'*** sake)

10. **Can't "Practice Law Without a License"**

9. **Can't Lawfully Advise on Compliance With Federal or State Law, Regulations, or Common Law**

8. **Can't Offer Your Customers Attorney-Client Privilege Protection**

7. **Can't Offer Your Customers "Advice of Counsel Defense"**

6. **Helps Reduce *YOUR* Potential Legal Liability**

TOP TEN Reasons to Have a Law Firm Involved (cont.)

5. **Someone Else to Blame if Not Current on All Federal, State, Common Law & International Legal Developments**

4. **Contracts That Make You as "Bulletproof" as Possible (including LOAs)**

3. **To Fight With The Other Guy's Lawyer**

2. **In On the Takeoff/In On the Landing**

1. **You DO NOT Want to Be This GUY:**

Sworn, Public Testimony Before the Honorable Royce Lamberth

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA
ELOUISE PEPION COBELL, et al., :
:
Plaintiffs, : Civil Action No. 96-1285
:
v. : Washington, D.C.
: Thursday, May 5, 2005
SECRETARY OF THE INTERIOR : 10:34 a.m.
et al., :
:
Defendants. :
:
. x
DAY 3 - AM SESSION
TRANSCRIPT OF EVIDENTIARY HEARING
BEFORE THE HONORABLE ROYCE C. LAMBERTH
UNITED STATES DISTRICT JUDGE

Sworn, Public Testimony Before the Honorable Royce Lamberth

Q. What is your understanding of what limitations were imposed on you that a hacker who is not operating in accordance with the Rules of Understanding would not have to following, if you could please identify that?
A. That would basically involve any type of modification of the system which involves like adding back doors, you know, adding Trojans, that would allow access at a later date, altering log files, or anything, you know, intended to cover up activity.
Q. So does that type of activity enhance the ability of a hacker to continue operations throughout a system that was able to be penetrated?
A. It can, yes.

Sworn, Public Testimony Before the Honorable Royce Lamberth

Q. Is it used generally by hackers if they are intent on obtaining information in a system, do you know?
A. It is commonly used.
Q. It is commonly used, and what are the -- does it open up new systems that were not identified? What are the consequences of using these other methodologies?
A. It would basically provide another avenue to access those systems in the event that, you know, they might have been detected, or it might, you know, in the case of altering or removing logs, it might keep the intrusion from being detected.
Q. And is it also a common practice for hackers to either disable or try and damage a system to distract any of the efforts that are going on throughout the system that has been penetrated?
A. In extreme cases it is possible, yes.

Sworn, Public Testimony Before the Honorable Royce Lamberth

- You can find this -- ***and 9.5 MORE DAYS of this type of public testimony at:***

http://www.indiantrust.com/index.cfm

- Your proprietary methods -- likely not protected in court
- Virtually impossible to resist court subpoena to testify, ***unless----***
- ***Your Customer*** has retained you via a law firm for ***legal advice as to compliance with federal or state laws***

Selecting Your Lawyers

- **Well regarded in the professional community?**
  - **www.martindale.com**
  - **Look for "AV Rated"**
- **Provable expertise in information security law**
- **Published in this area?**
  - **Example: Forthcoming Syngress Publication:**

    "Network Security Evaluation Using the NSA IEM"
  - **www.bookpool.com**
- **Trained/certified in recognized methodology**
  - ***For example----------***

Training and Rating Program

INFOSEC Assessment Methodology (IAM)
INFOSEC Evaluation Methodology (IEM)
Certified Individuals

Bryan Cunningham,
bc@morgancunningham.net

The following individuals successfully completed the NSA-sponsored IAM or IEM course on the date indicated. An individual's placement on this list does not constitute an endorsement, recommendation or warranty of his/her services on the part of NSA or any other government agency, nor does it imply any confirmation of an individual's experience level or ability. This web page is merely intended to distribute contact information of individuals who have successful passed the IAM or IEM courses. Listed individuals are responsible for the accuracy of contact information.

If you have taken and passed the NSA INFOSEC ASSESSMENT METHODOLOGY (IAM) and/or INFOSEC Evaluation METHODOLOGY (IEM) certification class(es) in the past and would like your name on the list, please mail the IAM Release Form or IEM Release Form to:

National Security Agency / Suite 6786
Attention: IATRP
9800 Savage Road (FANX I)
Fort George G. Meade, Md. 20755-6786

Corporate Strategies for Mitigating Liability

- Allegations in recent lawsuits
- What can we learn from them?
- Why even best efforts of in-house IT and InfoSec experts probably won't be enough

Corporate Strategies for Mitigating Liability

- Fully understand the risks
- Fully understand (with advice of expert counsel) the legal environment
- Outside, third-party assessments
- Using contracts to protect information

Corporate Strategies for Mitigating Liability

- Make sure your standards-of care assessments keep up with evolving law
- Plan for the worst
  - Crisis management planning
  - Crisis communication
- Consider Insurance

Topics to Cover in Information Security Consulting Contracts

WHAT

- Description of security service and business model
- Definitions of terms used in contract
- Description of the specific project
- Assumptions, representations, and warranties
- Boundaries and limitations
- Identification of deliverables

Topics to Cover in Information Security Consulting Contracts

WHO

- Statement of parties to agreement
- Authority of signatories
- Roles and responsibilities of each party
- Non-Disclosure & secrecy agreements
- Assessment personnel
- Crisis management and public communications
- Indemnification/duty to defend
- Ownership and control of information
- Intellectual property and licenses

Topics to Cover in Information Security Consulting Contracts

WHEN

- Timeline for completing deliverables
- Estimated dates of briefings (if any)
- Timeline for any follow-up work
- Actions or events that could affect the schedule

Topics to Cover in Information Security Consulting Contracts

WHERE

- Physical locations
- Logical locations
- Special caution for traversing the Internet
- Special caution where any part of locations are overseas

Topics to Cover in Information Security Consulting Contracts

HOW

- Methodology
- May want to break complex projects up into phases
- May want separate addendum for technical detail
- Don’t use technical jargon or slang

Topics to Cover in Information Security Consulting Contracts

HOW MUCH

- Fees and costs
- Billing methodology
- Payment expectations and schedule
- Rights and procedures to collect payment
- Insurance for potential damage during evaluation

Topics to Cover in Information Security Consulting Contracts

When Something Goes Wrong

- Governing law
- "Acts of God"
- When agreement is breached and remedies
- Liquidated damages
- Limitation on liability
- Survival of obligations
- Waiver and severability
- Amendments to contract

Where the Rubber Meets the Road: Why Letters of Authorization Are Your Friends

- **What is a "Letter of Authorization?"**
- **Example of how it works**
- **Why it's so important to protect information security consultants *and* their customers**
- **Special requirements for traversing the Internet**
- **Consider making LOA a separate agreement**

REMINDER: This Briefing ***Is Not Legal Advice***

- Provides an overview of policy and legal issues important to information security professionals
- We *cannot* provide legal advice unless in a retained, legal relationship with specific clients
- You ***cannot rely on these suggestions*** as legal advice
- Following suggestions in this briefing *does not create* any legal defense
- Information security professionals are *strongly urged* to retain qualified and experienced legal counsel

Morgan & Cunningham LLC

bc@morgancunningham.net

forrest@morgancunningham.net

(303) 743-0003