Sean L. Harrington
J.D., MCSE, CISSP, CSOXP, CHFI, CCFP

“Closing the Gap: Information Security and Legal”

May 16, 2016
Presenter Background

- Chair, data security and privacy practice, Pasky Gruber law firm
- 13 years in the banking industry (software development, information security, and public policy); last year in healthcare industry
- Digital forensics examiner in private practice since 2007
- Admitted to the practice of law in California and Wisconsin
- Certifications: CCFP, MCSE, CISSP, CHFI, and CSOXP
- Provides information security and HIPAA audits and policy writing for health care providers
- Licensed by the Texas Private Security Bureau (to practice digital forensics)
- Served on the board of the Minnesota Chapter of the High Technology Crime Investigation Association, and leadership roles in the FS-ISAC; the Financial Services Roundtable’s legislative and regulatory working groups; the Cyber working groups of SIFMA, the U.S. Chamber of Commerce, and the American Banking Association
- Current member of InfraGard, council member of the Minnesota State Bar Association’s Computer & Technology Law Section, and Fellow of the National Cybersecurity Institute
- Teaches computer forensics for Century College (Minnesota)
- Authored a chapter on the Code of Ethics for the Official (ISC)²® Guide to the Cyber Forensics Certified Professional CBK®, and until recently was an authorized (ISC)²® instructor
- Published several law reviews and trade articles on cyber security and ethics
This presentation is based upon the presenter’s scholarly works, and is intended to promote discussion and innovation. This presentation is not intended to convey legal advice; attendees should not act or refrain from acting based upon the presenter’s oral or written statements.
Overview

I. Opportunities for collaboration between Information Security and Legal

A. Contracting

B. Policy drafting

C. Dealing with regulators

D. Dealing with other third parties (e.g., vendors, partners, customers, etc.)
   1. in privity of contract (contractual obligations and dealings)
   2. understanding obligations and duty of care in infosec operations
      a. negligence
      b. tort
      c. ethics

E. Attorney-client privilege imposed on certain matters

F. litigation hold procedures

G. Compliance with the law in discharge of duties (e.g., CFAA, ECPA, etc.)
   1. Need for infosec practitioners to understand where the law applies
   2. Need for legal counsel to understand infosec activities
II. Strategies for improving relations and communications between IS and Legal

A. Effective communications techniques

1. reduce things to writing, unless counsel directs not to create a record

2. use concise, plain language free from unnecessary technical jargon

3. impose deadlines on when responses are needed and what is needed

B. Ensure joint representation in steering committees, governance committees, and other groups to bring both departments together in continuing collaboration
C. Seek out opportunities to review contracts, security addendums to contracts, statements-of-work, litigation hold memoranda, and other documents prepared by counsel. Although some attorneys are resistant to criticism, many are unfamiliar with correct terminology and infosec concepts. Because words are important in contracting, your expertise in helping to draft accurate language is invaluable.

D. Seek out opportunities to develop rapport with one or more associate counsel. If the relationship becomes close and collaborative, make yourself available to educate them on infosec topics — many attorneys are eager to expand their portfolio of knowledge.

E. Follow infosec-related court cases reported on infosec blogs, newsletters, and fora, and share important developments with counsel. (Unless there is dedicated cybersecurity counsel, most in-house counsel aren't keeping up with latest caselaw developments in encryption, employee electronic monitoring, web traffic monitoring, CFAA, ECPA, etc.).
F. Develop discernment as to when to reach out to counsel. As examples:

1. apparent violations — whether observed acts or existing or proposed practices — of law, regulations, ethical standards, corporate policies, contractual obligations, or other situations appearing to create legal liability (tort, negligence, contract, privacy, etc.)

2. Any need to understand or interpret legal obligations imposed on a workforce member or the organization by statute, regulation, or contract (and to avoid unauthorized practice of law ("UPL")), or to report UPL.

3. Recognizing UPL - refuse to perform work that appears to be "legal" in nature, even if delegated by counsel due to his or her reluctance to deal with infosec subject matter (this scenario may require escalation)
Exercise

Scenario A: Ass’t general counsel asks you to review infosec language in contract with a vendor providing managed services. Only language states that vendor must use, “Commercially reasonable, industry standard best practices.” In an e-mail reply, how do you respond?

Scenario B: You are the manager of a small team of penetration testers for your company. One of your team members states that he has successfully established attribution for a recent infiltration and has the ability to obtain root access of what he believes is the command-and-control server for the attacker’s bot-net. May he proceed to gather intelligence and/or sabotage the putative attacker’s server?
Digital Evidence

Case types: contract disputes, labor disputes, divorce and child custody, orders for protection, cyberstalking, corporate espionage, insurance fraud, you-name-it!

“Digital evidence is information of probative value that is stored or transmitted in a binary form.” (SWGDE, 1998)

Courts have allowed the use of: e-mails, Digital photographs, ATM transaction logs, Spreadsheets, Computer memory, Global Positioning System etc., Digital evidence is often ruled inadmissible by courts because it was obtained without authorization, or because its authenticity or integrity is called into question

Hearsay usually not an issue for an examiner: computer-generated logs are not hearsay; statements within e-mails, journals, etc., may be, but this is for the attorney working the case to sort
Evidence Must Be:

Relevant, *i.e.*, 
- material (directed toward a matter in issue); and
- probative (tends to prove or disprove a matter at issue).

If the evidence is both material and probative, it is relevant, and it is admissible unless some exclusionary rule applies.

Authentic
Rules of Civil Procedure, as relevant to information security practitioners (such as digital forensics examiners), define roles and responsibilities of investigators, forensic examiners and experts, court-appointed third party neutrals, special masters, protection for draft reports, among other things.
Federal Rules of Evidence

Article I: General Provisions

Article II: Judicial Notice

Article III: Presumptions in Civil Actions and Proceedings

Article IV: Relevancy and it’s Limits

Article V: Privileges

Article VI: Witnesses
Article VII

Rule 702 - Opinions and Expert Testimony
• A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
  a) the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
  b) the testimony is based on sufficient facts or data;
  c) the testimony is the product of reliable principles and methods; and
  d) the expert has reliably applied the principles and methods to the facts of the case.

Rule 703 – Bases Of An Expert’s Opinion
• An expert may base an opinion on facts or data in the case that the expert has been made aware of or personally observed.
Article VIII

Rule 801 – Hearsay

a) **Statement.** A person’s oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion.

b) **Declarant.** The person who made the statement.

c) **Hearsay.** “Hearsay” means a statement that:
   1) the declarant does not make while testifying at the current trial or hearing; and
   2) a party offers in evidence to prove the truth of the matter asserted in the statement.

• Rule 803 – Exceptions To The Rule Against Hearsay
  a. **Records of a Regularly Conducted Activity**
     1) the record was made at or near the time by someone with knowledge or transmitted;
     2) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
     3) making the record was a regular practice of that activity
Article IX

Rule 901: Authenticating Or Identifying Evidence

• In General – The proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is

Distinctive Characteristics and the Like

Evidence About a Process or System
Federal Rules of Evidence (cont.)

Article X: Original Document Rule
• applies when a party seeks to prove the contents of documentary evidence proffered to be admitted as evidence.
• If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original". Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule.
• where the original is not available, an acceptable excuse for the absence of the original must be supplied

Article XI: Miscellaneous Rule
Federal Rules of Evidence (cont.)

Attorney Client Privilege

Work Product Doctrine
# Classifications of Crimes

<table>
<thead>
<tr>
<th>Felonies</th>
<th>Crimes against persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misdemeanors</td>
<td>Property crimes</td>
</tr>
<tr>
<td><strong>Malum in se</strong></td>
<td>Inchoate crimes</td>
</tr>
<tr>
<td><strong>Malum prohibitum</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Malum in se* and *Malum prohibitum* are categories of criminal law that distinguish between crimes against persons and property crimes.
Elements of Crimes

The elements of the crime need to be present or there is no crime: (1) *actus reus*, (2) *mens rea*, (3) concurrence, and (4) both actual and proximate causation.

- **Prohibited Act** (*Actus reus*)
- **Criminal State of Mind** (*Mens rea*)
  - *intent*
    - purposeful or knowing
    - none required for strict liability
    - general intent
    - specific intent
    - malice
    - negligence and recklessness
Crimes: Burden of Proof

Prosecution must prove each and every element of the crime beyond a reasonable doubt.
Presumptions are disallowed; the jury may, however, draw permissive inferences.
Judicial notice: not binding on the jury.
Types of Torts

Intentional torts
  • *prima facie* elements: volitional act, intent, causation, damages
  • against the person (e.g., assault, battery, defamation, IIED)
  • against property

Negligence
  • elements: duty, breach, actual & proximate causation, damages

Strict liability

Products liability
Contract Issues

Governed by the common law or UCC?
Formation issues:
• bilateral or unilateral?
• evidence of valid offer, valid acceptance, and sufficient consideration, and possible defenses (statute of frauds, incapacity, duress, undue influence, fraud, mistake, illegality)
Statute of frauds: requires a writing for the transfer of interest in real property estates, contracts that cannot be performed in less than one year, goods in excess of $500
Issues regarding breach:
• promise vs. covenant or promise vs. condition
• part or substantial performance
• defenses to failure to perform: frustration of purpose, impracticability, impossibility, voluntary disablement, wrongful prevention (hindrance), unconscionability, inter alia.

Breach
• That duty was breached and endangered the health and safety of the plaintiff

Causation
• The plaintiff suffered injury in some form

Damages
• The plaintiff’s injuries were caused by the negligence of the
Examples:

• GLBA
• HIPAA
• FFIEC (e.g., requirements codified in C.F.R. that boards of financial institutions must oversee and approve the information security program)
• FINRA/SEC targeted assessments (cybersecurity sweeps)
• FTC (e.g., Wyndham hotels)
• State (e.g., data breach notification)
Expert Witnesses

An expert witness is someone with knowledge of or experience in a particular field or discipline beyond that to be expected of a layman. An expert witness is paid for the time it takes to:

• form an opinion
• support that opinion during the course of litigation

An expert witness is not paid for the opinion given, and still less for the assistance that opinion affords the client’s case.

This can include scientists, criminalists, forensic technicians, and identification technicians.

1 Ref: Expert Witness Institute (EWI) http://www.ewi.org.uk/membership_directory/whatisanexpertwitness
Expert Advisor

Straying from acting as an expert witness into advising the client makes one an expert advisor.

As an expert advisor, immunity from suit may be limited.
The Adam Walsh Act

Requires defense experts to perform analysis in LE facilities. If contraband is discovered in civil case, examiner must immediately cease all work, summon law enforcement, and take no further action.
Privacy

Privacy laws affect corporate investigations more than they do criminal investigations, except Fifth Amendment Right Against Self Incrimination and Fourth Amendment Unreasonable Searches and Seizures (to be discussed soon).

Health Insurance Portability and Accountability Act (HIPAA): governs the use and disclosure of individuals’ health information by subject entities.” The Privacy Rule is intended to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.
Gramm-Leach-Bliley Act: requires financial institutions to protect information collected about individuals, and prohibits disclosure of their customers' account numbers to non-affiliated companies relative to telemarketing, direct mail marketing or other marketing through e-mail. Payment Card Industries (PCI DSS 2.0): contractual standard, not law, that prescribes information security controls and processes (e.g., penetration testing, vulnerability assessments, risk assessments, inter alia). Note, several states (e.g., MN, WA, MA, NV) have substantively adopted the standard as law.

Many states (e.g., CA and MN) have mandatory data breach notification statutes
Amendment IV / Warrants

“The Right of the people to be secure in their **persons**, **houses**, **papers**, and **effects**, against **unreasonable searches** and **seizures**, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

State constitutions have similar language

*N.B.: many state constitutions accord greater Bill-of-Rights protections than the Federal Constitution.*
State Action doctrine

- The 4th Amendment applies ONLY to the Government.
- Private parties (e.g., computer repair shops, IT administrators) not subject to the 4th Amendment.
- Experts examining a computer independently of any contact with law enforcement are not a state actor.

However . . .

If an expert is responding to a request from law enforcement, he or she becomes an agent (deputized).

If the officer has informed him or her that a warrant would be necessary (for the officer), the expert would need the same warrant that the officer would!
A search is deemed reasonable if it does not violate a person’s “reasonable” or “legitimate” expectation of privacy.

“Reasonable” expectation of privacy is determined by the courts by balancing a person’s subjective expectation of privacy vs. what society is prepared to recognize as reasonable.
SEARCHES AND SEIZURES

• No bright line rule for “Reasonable Expectation of Privacy”

• A person’s home, heat from your home, conversations in a closed telephone booth, and opaque closed containers are considered areas where a person does have a reasonable expectation to privacy by the courts.
SEARCHES AND SEIZURES

- Open fields, trash put out for collection, houses where the person has entered illegally are considered areas where a person does not have a reasonable expectation of privacy.
- Some courts have reasoned that electronic devices, including computers, are similar to opaque closed containers, and accessing these devices is like opening the container.
- Because individuals generally enjoy a reasonable expectation of privacy in closed containers, it is assumed that they enjoy the same when it comes to the data on their computer.
Entitled to Privacy

- Home computer shared with spouse where login is password-protected and not disclosed to spouse
- Flash drive kept in pocket for personal use
- Cell phone for personal use (in most states)
- Laptop carried around for personal use
NO PRIVACY

- Abandoned discs or drives
- Images on the monitor (DEPENDS!)
- Computers or devices shared among many
- Company computers (POLICY)
- Web sites available to the public
- E-Mail received by another party
- Chat posted to a public site
Warrant Requirement Exceptions

- Warrant less searches can be reasonable and lawful under a few court recognized exceptions:
  - Consent
  - Exigent Circumstances
  - Plain View
  - Search Incident to Arrest
  - Inventory Searches
  - Border/International Searches
CONSENT

• Does the person have authority or capacity to grant consent?
• Must be voluntary
• Scope of consent
• Person must have ability to revoke consent
• Parents, spouses, third parties
• System Administrators
EXIGENT CIRCUMSTANCES

• Police can search without a warrant if the circumstances “would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts.”
EXIGENT CIRCUMSTANCES
Factors:

• Degree of urgency
• Amount of time necessary to obtain a warrant
• The possibility of danger at the site
• Suspects are aware police are on their trail
• Evidence is evanescent, or about to be removed or spoliated
EXIGENT CIRCUMSTANCES

• Often arises in computer searches due to data being easily perishable
• Generally, a computer or electronic device can be seized under exigent circumstances, however, rarely can it be searched under this exception.
• Exigency must be tied to the facts of the case
Officer must lawfully be in a place and observe and access evidence that is immediately apparent.

Plain view does not allow an investigator to open a file to “view” it.

United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999) – officer searching for evidence of narcotics accidentally opens a jpg containing child pornography, but continues to now look for child pornography: outside the scope of the warrant.
SEARCH INCIDENT TO LAWFUL ARREST

• Pursuant to a lawful arrest, an officer may conduct a full search of a person and any “lunge, reach or grab” area around that person – including vehicles.

• Electronic devices are becoming smaller now and can be carried on someone’s person:
  • Pagers: YES
  • Cellphones: Yes, in some states
  • PDAs, Flash Drives: Follow the case law. Note, the capacity of some of these devices may lead the courts to scrutinize searches under this exception because it is more invasive.
INVENTORY SEARCH

Allows officers to conduct a warrantless search of a person’s items that they have seized.

Must be in policy and must be routine.

It is not investigatory in nature – it is only to protect the person’s property (and officer safety) while it is in police custody.

Generally, there is no time that a computer may be searched under this exception.
BORDER SEARCHES

• Routine, random warrantless border searches have been recognized by courts as lawful under the 4th Amendment.
• This would include physical borders, ship ports, and airports.
• See, e.g., United States v. Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000) (border agents may search computer disks and electronic equipment as part of their job duties with no reasonable suspicion needed).
WARRANT VS. NO WARRANT

• Searches conducted with a warrant presumed to be lawful; those without a warrant presumed to be unlawful
• Although it may be permissible under exigent circumstances to seize a computer without a warrant, it is rare that LE may search a computer under exigent circumstances.
• When in doubt, obtain a warrant!
• If evidence of a second, unrelated crime is found on a warrant, LE must stop immediately and seek another warrant.
EXCLUSIONARY RULE

- Evidence acquired directly or indirectly by an unconstitutional search, seizure, or arrest generally is inadmissible at a criminal trial as proof of guilt.
- Applies to both state and federal actions.
- Rule purpose: to deter police misconduct.
- If a computer is seized in violation of the 4th Amendment, ALL data on that computer will be inadmissible in court.
EXCLUSIONARY RULE (Cont.)

• Penalty under the exclusionary rule is suppression of the evidence and ALL other evidence that is the “fruit” of the tainted evidence “Fruit of the Poisonous Tree”
• Three exceptions: (1) Independent Source Doctrine; (2) Inevitable Discovery Doctrine; and (3) Good Faith
• Because the Fourth and Fifth Amendments apply only to government action, courts will not exclude evidence obtained by a private party acting independently of the police
Many states have counterpart statutes, some of which contain more specific language and are less antiquated.

Computer Fraud and Abuse Act of 1986
• Provides both civil and criminal penalties for violation

Electronic Communications and Privacy Act of 1986
• Provides both civil and criminal penalties for violation
• Title I: Wiretap Act
• Title II: Stored Communications Act
• Title III: pen register and trap and trace devices

Privacy Protection Act of 1980
CFAA

- Directed at criminal computer hacking (more on this later!)
- Prohibits computer intrusions — accessing computers “without authorization,” or “exceed[ing] authorize[d]” access, which statutory phrases have been the continuing subject of appellate review.
- Private parties who can show “damage or loss” in excess of $5,000, which can include the cost of hiring a forensic examiner plus his or her assessment of the damage caused to the victim’s computer or business, can sue.
- The Government can pursue felony charges if damages are in excess of $5,000
- House Judiciary Committee considering augmenting the Act — all offenses would be felonies
ECPA — Title I

• Update of the original wiretap law of 1968
• Prohibits interception, disclosure, or use of wire, oral, and electronic communications in transit
  • must be contemporaneous with transmission
  • examples: e-mail, text/video messaging, keystrokes (some courts)
• Prohibits public Internet carriers from disclosing content of in-transit e-mail
ECPA — Title II (Stored Communications Act)

• Applies to ISPs. Inapplicable to private companies’ internal e-mail systems.

• Restricts Government access to customer and subscriber information and records

• Providers may disclose protected information if:
  • Consent is given by the sender, an addressee, or the recipient
  • Content was inadvertently obtained and appears to contain evidence of the commission of a crime
SCA

- Subscriber Information – Subpoena or Search Warrant
- Content of E-Mail:
  - Less than 180 days = Search Warrant (No Notice to Subscriber)
  - More than 180 days = Search Warrant (No Notice) OR subpoena or court order (With Notice to Subscriber)
SCA (cont.)

• Exceptions to the Notification Rule — notification may be delayed up to 90 days if it may cause:
  • danger to the life or physical safety of an individual.
  • a flight from prosecution.
  • destruction of or tampering with evidence.
  • intimidation of potential witnesses.
  • serious jeopardy to the investigation.
  • undue delay of a trial.
• LE may send a formal written request to a provider to “freeze” an account while a subpoena or search warrant is being applied for or drafted
• These “Freezes” sometimes notify the target that their account is being acquired by government agents. If secrecy is an issue, talk with the provider about their policies with freezing an account.
PPA

- Purpose: to limit searches for materials held by persons involved in First Amendment activities and not themselves suspected of criminal activity being investigated
- Protects “Work Product Materials” and “Documentary Materials” that is original work that anyone in possession of it intends to publish
- Does not protect illegal material (pirated software, stolen credit card numbers, child pornography, etc.)
- Liability: Both federal and state agencies and their employees may be sued under this act for violations (in most circumstances)
Work product materials are defined as materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or the means of committing a criminal offense—and—

- are prepared, produced, authored, or created, by the person possessing the materials, or any other person, in anticipation of communicating the materials to the public;
- are possessed for the purposes of communicating such materials to the public; and
- include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material.
Defined as encompassing materials upon which information is recorded, and includes, but is not limited to:

- photographs
- motion picture films
- negatives
- written or printed materials
- video tapes
- audio tapes
- other mechanically, magnetically or electronically recorded cards, tapes, or discs

Excludes illegal material
WARRANTS AND THE PPA

• Work Products and Documentary Material protected under the PPA may be searched and seized under warrant in order to:
  • Prevent death or serious injury
  • To search for evidence of a crime held by a suspect of that crime
WARRANTS AND THE PPA

• Additionally, agents are allowed to get a warrant for Documentary Materials if one of the following is true:
  • there is reason to believe that the giving of notice by a subpoena would result in destruction, alteration, or concealment of the materials
  • the materials have not been produced in response to a court order directing compliance with a subpoena, and all appellate remedies have been exhausted; or there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpoena would threaten the interests of justice.

• Seek legal advice when dealing with items protected under the PPA
PPA (cont.)

- PPA appears to apply broadly (electronic bulletin boards)
- PPA applies only when materials are possessed by a person reasonably believed to have a purpose to disseminate to the public “a newspaper, book, broadcast, or other similar form of public communication.”
- There must be some indication the person intended at that time to disseminate the material.
PPA Issues

• If it is known that PPA materials may be seized on a computer, PPA language should be placed in the warrant specifying that PPA protected documents will be returned without delay. If documents will not be returned immediately, language should be built into the warrant allowing for a delay before searching to allow the owner of the material time to contest the search in court.

• If material is found that could be protected under the PPA, that material should be returned to the owner immediately, and the prosecutor notified.
SEARCH WARRANTS

• Law enforcement officers must draft two documents to obtain a search warrant
  • An affidavit, a sworn statement that (at a minimum) explains the basis for the affiant's belief that the search is justified by probable cause.
  • The proposed warrant, typically a one-page form, plus attachments, incorporated by reference, that describes with particularity the place to be searched, and the persons or things to be seized.
SEARCH WARRANTS

• Warrants typically are drafted by prosecutors. They must include in detail:
  • The property or persons that are to be seized
  • The property or persons that are to be searched
  • The probable cause to issue the warrant and the violations in the criminal code involved
  • In the affidavit, support of the probable cause and any other practical and legal strategies and considerations that may govern the execution of the search
PROBABLE CAUSE

• “Probable Cause” = facts and circumstances sufficient to warrant a reasonable person believing that it is more likely than not that the proposed search is justified.

• It is less than “beyond a reasonable doubt” but more that “reasonable suspicion”.

• Trustworthy evidence is required that the particular items to be searched or seized—
  • are connected with criminal activity; and
  • will be found in the place to be searched.
SEARCH WARRANTS

• Warrants must be signed by a neutral or detached judge, magistrate, or court commissioner.
• Law enforcement typically has a prosecutor and a judge on call 24 hours a day to prepare and review warrant requests.
WARRANT CONSIDERATIONS

• If a third party expert is to be involved in the warrant, this must be specified in the warrant. The involvement of this expert must be detailed in the affidavit and his or her duties during the warrant limited to their assigned role.

• Will a “No-Knock” warrant be advised?
NO KNOCK WARRANTS

• During the execution of a warrant, police must typically “knock and announce” their presence.
• A “No Knock” authorization in a warrant may be applied for if:
  • The safety of the public or the officer would be put at risk by knocking and announcing
  • Evidence would be destroyed and inhibit the investigation
• Due to volatility of computer evidence, it may be prudent under certain circumstances to apply for a “no-knock” warrant.
Electronic Discovery

Excerpted, in pertinent part, from Fed.R.Civ.P. (b):

Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.
Active Defense - Terms

- Active Defense
- Hack Back
- Offensive Counter Measures ("OCM")
- Retaliatory Hacking

Protecting and defending electronic information and assets in and beyond one’s own network.
Federal Statutory Prohibitions

• Computer Fraud and Abuse Act of 1986
  • Provides both civil and criminal penalties for violation
• Electronic Communications and Privacy Act of 1986
  • Provides both civil and criminal penalties for violation
    • Title I: Wiretap Act
    • Title II: Stored Communications Act
    • Title III: pen register and trap and trace devices
• Many states have counterpart statutes, some of which contain more specific language and are less antiquated.
CFAA

- Directed at criminal computer hacking
- Prohibits computer intrusions — accessing computers “without authorization,” or “exceed[ing] authorize[d]” access, which statutory phrases have been the continuing subject of appellate review.
- Private parties who can show “damage or loss” in excess of $5,000, which can include the cost of hiring a forensic examiner plus his or her assessment of the damage caused to the victim’s computer or business, can sue.
- The Government can pursue felony charges if damages are in excess of $5,000
- House Judiciary Committee considering augmenting the Act — all offenses would be felonies
ECPA — Title I

- Update of the original wiretap law of 1968
- Prohibits interception, disclosure, or use of wire, oral, and electronic communications in transit
  - must be contemporaneous with transmission
  - examples: e-mail, text/video messaging, keystrokes (some courts)
- Prohibits public Internet carriers from disclosing content of in-transit e-mail
Privacy

• Examples:
  – CA and MN
    • Data handling
    • Data Breach Notification
  – PCI DSS
  – Gramm-Leach-Bliley Act: requires financial institutions to protect information collected about individuals, and prohibits disclosure of their customers' account numbers. See also FFIEC Examination Book.
ECPA — Title II ( Stored Communications Act )

• Applies to ISPs. Inapplicable to private companies’ internal e-mail systems.
• Restricts Government access to customer and subscriber information and records
• Providers may disclose protected information if:
  • Consent is given by the sender, an addressee, or the recipient
  • Content was inadvertently obtained and appears to contain evidence of the commission of a crime
Ethics

Codes of Conduct describes the expected behavior of members of an association or practitioners of a profession, and generally seek to protect the organization or profession from the consequences of bad behavior of its members.

- ABA Model Rules 1.2, 5.3, 8.4(c)
- (ISC)² Code of Ethics Preamble*
- (ISC)² Code of Ethics Cannons**
- Model Rules
Approaches

• Beaconing
• Sinkholing
• Honeypots
• Disinformation
• Retaliatory Hacking
## Risk Matrix

<table>
<thead>
<tr>
<th>Approaches</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beaconing</td>
<td>Legal</td>
</tr>
<tr>
<td>Threat Intelligence Gathering</td>
<td>Ethical</td>
</tr>
<tr>
<td>Sinkholing</td>
<td>Escalation</td>
</tr>
<tr>
<td>Honeypots</td>
<td>Misattribution and collateral damage</td>
</tr>
<tr>
<td>Retaliatory Hacking</td>
<td>Goodwill &amp; reputation</td>
</tr>
</tbody>
</table>
Justifications

Theories advanced to justify retaliatory hacking:

• Recapture of chattels
• private necessity
• Castle doctrine
• private security guard doctrine
Alternatives to Hack Back

- **Preventive**: Private entities’ collaboration with ISPs and industry partnerships to combat; Intelligence sharing and gathering (ISACs); perimeter hardening
- **Detective**: tools; know your network traffic; behavioral anomaly analysis; parse your logs
- **Corrective**: collaboration with government and other private corporations: (e.g., takedowns of Citadel, Zeus)
- **Corrective**: cyber legislation
- **Risk transfer**: (outsourcing, cyber insurance)
References


Framework for Improving Critical Infrastructure Cybersecurity
Presidential Executive Order 13636: “Improving Critical Infrastructure Cybersecurity”

• “It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

• President Barack Obama
  • Executive Order 13636, Feb. 12, 2013

• The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure

• Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work
As Directed in the EO, the Cybersecurity Framework ...

- Includes a set of existing standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations.
FRAMEWORK COMPONENTS

- Framework Core
- Framework Profile
- Framework Implementation Tiers
Framework Core

Cybersecurity activities and informative references common across critical infrastructure sectors and organized around particular outcomes:

- Identify
- Protect
- Detect
- Respond
- Recover

Framework Profiles

- Aligns the Framework Core to business requirements, risk tolerance, processes, and procedures.

A profile can represent the current state and desired target state (*i.e.*, a roadmap for reducing cybersecurity risk).
Framework Core → Profile[s]

Cybersecurity activities and informative references common across critical infrastructure sectors and organized around particular outcomes:

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>CATEGORY</th>
<th>SUBCATEGORY</th>
<th>INDUSTRY STANDARDS IN ALIGNMENT</th>
</tr>
</thead>
</table>
| PROTECT (PR) | Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. | PR.DS-1: Data-at-rest is protected | CCS CSC 17  
COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06  
ISO/IEC 27001:2013 A.9.1.1  
NIST SP 800-53 Rev. 4 SC-28  
IEC/ISA 62443-2-1:2010 4.3.2.5, 4.3.2.6, 4.3.3.3, 4.3.4.3, 4.3.4.4, 4.3.4.5 |
Framework Core → Profile[s] (cont.)

- 22 categories; 98 subcategories
- Utilizes common taxonomy
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IMM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

Framework Core $\rightarrow$ Profile[s] (cont.)

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Sub-category</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| IDENTIFY (ID) | | ID.AM-1: Physical devices and systems within the organization are inventoried | - CCS CSC 1  
- COBIT 5 BAI09.01, BAI09.02  
- ISA 62443-2-1:2009 4.2.3.4  
- ISA 62443-3-3:2013 SR.7.8  
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
- NIST SP 800-53 Rev. 4 CM-8 |
| | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy. | ID.AM-2: Software platforms and applications within the organization are inventoried | CCS CSC 2  
- COBIT 5 BAI09.01, BAI09.02, BAI09.05  
- ISA 62443-2-1:2009 4.2.3.4  
- ISA 62443-3-3:2013 SR.7.8  
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
- NIST SP 800-53 Rev. 4 CM-8 |
| | | ID.AM-3: Organizational communication and data flows are mapped | CCS CSC 1  
- COBIT 5 DSS05.02  
- ISA 62443-2-1:2009 4.2.3.4  
- ISO/IEC 27001:2013 A.13.2.1  
- NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 |
| | | ID.AM-4: External information systems are catalogued | COBIT 5 APO02.02  
- ISO/IEC 27001:2013 A.11.2.6  
- NIST SP 800-53 Rev. 4 AC-20, SA-9 |
| | | ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | COBIT 5 APO03.03, APO03.04, BAI09.02  
- ISA 62443-2-1:2009 4.2.3.6  
- ISO/IEC 27001:2013 A.8.2.1  
- NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 |
| | | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | COBIT 5 APO01.02, DSS06.03  
- ISA 62443-2-1:2009 4.3.2.3.3  
- ISO/IEC 27001:2013 A.6.1.1 |

Framework Tiers

• Describes how cybersecurity risk is managed by an organization:
  • Tier 1 – Partial
  • Tier 2 – Risk Informed
  • Tier 3 – Repeatable
  • Tier 4 - Adaptive

• NIST says, “Tiers do not represent maturity levels,” yet also says “Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.”
NIST’s proposed implementation roadmap

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze, and Prioritize Gaps
7. Implement Action Plan
Key Points about the Framework

• The Framework is:
  • a *framework*, not a prescription.
  • a flexible, adaptable tool.
  • a demonstration of a strong public-private partnership
  • a living document.

• In addition, the Framework, namely the roadmap between the current profile and the target profile has proven to be a useful vehicle for communicate cybersecurity requirements by operations to directors, and thus more likely able to procure CapEx funding
Concerns, Interpretation, and Socialization

• Parlance, Semantics, and Disagreement
  • NIST says the Core is “[N]ot a checklist of actions to perform.” Is not conducting a gap analysis from a current profile to a target profile a checklist? What is the distinction between “checklist” and “roadmap?”
  • NIST says, “Tiers do not represent maturity levels,” yet also says “Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.”
  • “conformance,” “compliance,” “confidence”
  • Complaints from the peanut gallery that the Framework is not voluntary
  • Will Framework adoption be considered a minimum standard of due care?
    – Recent suit against Target Corp. by several banks
    – Recent class action against Sony Pictures.
    – Patco Constrauction v. Peoples United Bank
What’s Next: Areas for Development, Alignment, and Collaboration

• The Executive Order calls for the framework to “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations”
• High-priority areas for development, alignment, and collaboration were identified based on stakeholder input:

  Authentication          Automated Indicator Sharing
  Conformity Assessment   Cybersecurity Workforce
  Data Analytics          Technical Privacy Standards
  International Alignment Supply Chain Risk Management
  Federal Agency Cybersecurity Alignment

Industry groups, associations, and non-profits can play key roles in assisting their members to understand and use the framework by: (1) Building or mapping sector specific standards, guidelines, and best practices to the framework; or (2) developing and sharing examples of how organizations are using the framework.

NIST is committed to helping organizations understand and use the framework, and has expanded its outreach and is working with DHS on its “C³” Voluntary Program (http://www.dhs.gov/about-critical-infrastructure-cyber-community-c³-voluntary-program)

• Share your framework experiences at cyberframework@nist.gov
• Participate through the National Cybersecurity Center of Excellence (NCCoE)
• Follow NIST’s cybersecurity activities at http://csrc.nist.gov