Logon Banners

Mr. Keelan T. Stewart

June 19th, 2019

NEbraskaCERT Cyber Security Forum

About the Speaker

- Education and Certification
  - BS, MS in Information Assurance, University of Nebraska Omaha
  - Certified Information Systems Security Professional, CISSP
  - GIAC Law of Data Security & Investigations, Gold Paper, GLEG Gold
  - HealthCare Information Security and Privacy Practitioner, HCISPP
  - GIAC Strategic Planning, Policy, and Leadership, GSTRT
- Experience
  - Information Security Analyst and Authorizing Official, Boys Town
  - Nuclear and Space Mission Systems Cybersecurity Analyst, U.S. Strategic Command
  - National and Nuclear Command and Control Enterprise and Solutions Architect

Agenda

- Introduction
  - Computer Crime Laws
  - Criminal Elements
- Logon Banner Elements
- Regulatory Requirements
- Drafting a Logon Banner

Disclaimer

- I am not an attorney.
- This presentation is for information only and should not be taken as legal advice.
- If you require legal advice on this topic, consult your attorney.

TL;DR

- “This computer is the property of [company]. Unauthorized access is prohibited.”
  - (Wright & Milone, 2017)
  - Ben Wright teaches SANS LEG523, Law of Data Security and Investigations

Introduction

Introduction

- Litigation surrounds cyberattacks
  - Victim is both plaintiff and defendant
- Logon banners
  - Reasonable, belt-and-suspenders
  - “No Trespassing” sign
  - Not the sole control (bank vaults)
- GIAC Gold Paper:
  - https://www.giac.org/paper/gleg/795/logon-banners/162031

Computer Crime Laws

Computer Crime Laws: 4th Amendment (1791)

- Right to Privacy
  - Government agents (US Constitution)
  - Agents acting on behalf of government (*Mapp v. Ohio*, 1961)
  - Telephone conversations (*Katz v. US*, 1967)
  - Stored electronic data (*US v. Heckenkamp*, 2007)
  - Electronic communications (*US v. Warshak*, 2010)
- Primary motivation for government logon banners is to reject any expectation of privacy

Computer Crime Laws:
The Communications Act (1934)

- Wiretapping telegraphs and telephones
  - Illegal for anybody (state laws, 1800s)
  - Not considered searches (*Olmstead v. US*, 1928)
- Divulging information from wiretaps
  - Part of an effort to regulate AT&T monopoly
  - Established expectation of privacy beyond physical locations

Computer Crime Laws:
Federal Wiretap Act (1968)

- Right to Privacy
  - From state governments (*Mapp v. Ohio*, 1961)
  - Searches of intangible property (*Katz v. US*, 1967)
- Legalizing Wiretaps
  - War on Drugs
  - Requires a warrant
  - Allows one party to record without consent

Computer Crime Laws:
The Computer Fraud and Abuse Act (1984)

- Authorized Access
  - Cold War, *WarGames*
  - Unauthorized access illegal
- Trespass to Chattels
  - Causes damages to owner, through denial or degradation
  - Civil tort
- Establishing when access is unauthorized is the principal issue addressed by implementing a logon banner

Computer Crime Laws:
Electronic Communication Privacy Act (1986)

- Right to Privacy
  - Personal communications, even in workplace
- Workplace Monitoring
  - May monitor performance, bona fide business purposes
  - Enforce company policy
- Acceptable use policies should address issues related to employee monitoring, not logon banners

Computer Crime Laws:
USA PATRIOT Act (2001)

- National Security Threats
  - Warrants may be issued without subject's knowledge
  - Information stewards (ISPs, aggregators) need not notify nor obtain consent for such requests

Computer Crime Laws:
Fair Trade Laws

- Unfair or deceptive acts or practices
  - How most organizations are regulated for cyber incidents
  - Not complying with self-imposed policies and procedures
    - Ex., Ashley Madison Privacy Policy

Computer Crime Laws:
State Privacy Laws

- Breach Notification Laws
  - All 50 states, DC, and 3/5 territories
  - Often require written policies

Criminal Elements

Criminal Elements: *Actus Reus* – Guilty Act

- Prosecuting a crime requires
  - Proving that a crime was committed
  - Proving that an individual(s) committed that crime
- Cybercrimes
  - Often easy to prove a crime was committed
  - Often not easy to prove who committed that crime
- It is not necessary to state the law in a logon banner – ignorance of the law is not a valid defense

Criminal Elements:
Mens Rea – Guilty Mind

- Criminal Intent
  - Technical skill may establish intent
  - Script kiddies may cause collateral damage
- Logon Banners
  - Help to establish criminal intent
  - Especially when coupled with an authentication mechanism

Logon Banner Elements

Logon Banner Elements: Ownership

- Legal Boundary
  - Crossing constitutes access, authorized or not
  - May require two statements for service providers
- Sample Language
  - “This computer is the property of [company].”
  - “This service is the property of [company x]. This computer is the property of [company y].”
  - “Computer” is most used in legislation and court findings

Logon Banner Elements: Prohibition

- Authorized Access
  - Establish what actions are permitted or not
  - Acceptable use policy may be more verbose
  - Limit over defining, which can create loopholes or omissions
- Sample Language
  - “Unauthorized access is prohibited.”

Logon Banner Elements:
Scope

- Boundary
  - Attempts to explicitly define the boundary
  - Implies things not listed are excluded
  - Better approach is to put logon banners on all access points
  - Not specifying reserves the right to argue scope later
- Sample Language
  - “…including all equipment, networks, devices, logs, etc.”

Logon Banner Elements: Audience

- Boundary
  - Attempts to explicitly define the audience
  - Implies people not listed are excluded
  - Better approach is to address requirements specific to a certain class of user (contractors, etc.) in the AUP
  - The ultimate audience of a logon banner is a judge and jury
- Sample Language
  - "…user, including employees, contractors, vendors, customers, etc."

Logon Banner Elements: Monitoring

- Expectation of Privacy
  - Attempts to explicitly nullify privacy
  - May be required for government agencies
  - Better approach is to address in acceptable use policy
- Sample Language
  - “…may be monitored, recorded, or subject to audit”

Logon Banner Elements: Enforcement

- Legal Recourse
  - Attempts to deter malicious activity
  - Better approach is to address in acceptable use policy
  - Not necessary to state that crimes may be prosecuted
- Sample Language
  - “…subject to disciplinary action, civil or criminal charges”

Logon Banner Elements: Evidence

- Expectation of Privacy
  - Attempts to limit legal liability
  - Organizations are subject to lawful subpoenas
  - Burden is on law enforcement with respect to claims of unlawful search and seizure, not organizations
- Sample Language
  - “…evidence may be provided to law enforcement”

Logon Banner Elements: Consent

- Expectation of Privacy
  - Attempts to establish legal contract
  - No consensus on standing of pop-up contracts
  - Bona fide consent requirements, such as monitoring, should be conveyed in a signed acceptable use policy
- Sample Language
  - “…by continuing, you consent to these terms”

Logon Banner Elements: Deterrence

- Legal Recourse
  - Attempts to deter malicious activity
  - No consensus on effectiveness, may challenge hackers
    - Did FBI anti-piracy warnings stop bootleg movies?
  - International criminals are often not usually not subject to the same laws anyway
- Sample Language
  - “…subject to fines, imprisonment, or both”

Regulatory Requirements

Regulatory Requirements: FISMA/NIST

- AC-8: System Use Notification
  - Ownership, prohibition, monitoring, consent
  - Agencies may require additional language
  - When not required, be brief and direct

Regulatory Requirements:
Nuclear Regulatory Commission

I UNDERSTAND AND CONSENT TO THE FOLLOWING:

I am accessing a U.S. Government information system provided by the U.S. Nuclear Regulatory Commission (NRC) for U.S. Government-authorized use only, except as allowed by NRC policy. Unauthorized use of the information system is prohibited and subject to criminal, civil, security, or administrative proceedings and/or penalties.

USE OF THIS INFORMATION SYSTEM INDICATES CONSENT TO MONITORING AND RECORDING, INCLUDING PORTABLE ELECTRONIC DEVICES.

The Government routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, or seize any communication or data transiting or stored on this information system.

Any communications or data transiting or stored on this information system may be disclosed or used in accordance with federal law or regulation.

REPORT ANY UNAUTHORIZED USE TO THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (301-415-6666) AND THE INSPECTOR GENERAL.

Regulatory Requirements:
Criminal Justice Information Systems

- FBI regulates CJIS, which extends to most local LEAs
  - Ownership, prohibition, monitoring, consent
  - Same as FISMA, NIST SP 800-53 AC-8

Regulatory Requirements: Financial and Retail

- Sarbanes-Oxley
  - Privacy policy but not logon banners
- Gramm-Leach-Bliley
  - Privacy policy but not logon banners
- PCI-DSS
  - Several security controls but not logon banners

Regulatory Requirements: Healthcare

- HIPAA/HITECH
  - Several security controls but not logon banners
- HITRUST Level 2
  - Ownership, prohibition, monitoring, consent (NIST)
- HITRUST Government Contractors
  - Ownership, prohibition, scope, monitoring, enforcement, evidence, consent, deterrence
- The Joint Commission
  - Several security controls but not logon banners

Drafting a Logon Banner

Drafting a Logon Banner: Identify Requirements

- Requirement Sources
  - Laws and Regulations
  - General Counsel
- Alternative Solutions
  - Acceptable Use Policy
  - Privacy Policy
  - A comforting pat on the back

Drafting a Logon Banner: Select Elements

- Always Have
  - Ownership and prohibition
- Select more only when required
- Default logon banner for most situations:
  - “This computer is the property of [company]. Unauthorized access is prohibited.” (Wright & Milone, 2017)

Drafting a Logon Banner: Review and Socialize

- Involve all necessary stakeholders
  - Legal, IT, HR, marketing, executives
- Address all concerns
  - Whether in banner, policy, or back pats
- Socialize with entire user base prior to implementation
  - Identify overlooked, unique situations
  - Inform of highly visible, persistent change

Conclusion

Conclusion

- Effective, inexpensive security control
  - Enhances ability to litigate computer crimes
  - Demonstrates you take security seriously
- Brevity is the soul of wit (Shakespeare, 1599)

Questions?