Using Accountability Theory to Reduce Unauthorized Data Access
A New Countermeasure to an Age-Old Problem

Gove N. Allen
Nicholas L. Ball

Information Systems Department
Marriott School of Management
Brigham Young University

Outline
1. The Problem of Unauthorized Access
2. Accountability Theory
3. Research Results
4. Future Research
Allina Video Here

Abuse of Power

Abuse of Authority

The problem of Unauthorized Data Access
Abuse of Power

Hacking is unauthorized access to system by outsiders to organizations.

- Jonathan James: Broke into NASA and DTRA stealing software worth millions. He was 16.
- Adrian Lamo: Hacked the New York Times, Microsoft, Yahoo!, and MCI WorldCom.
- Vladimir Levin: Hacked into Citibank and transferred $3.7 million to his own accounts.
- Kevin Poulsen: Hacked phone system of L.A. radio station KIIS-FM to win a Porsche 944.
- Kevin Mitnick: Hacked into DEC, IBM, Motorola, NEC, Nokia, Sun Microsystems, and others.
- Gary McKinnon: Disabled 2,000 U.S. Military Computers from Scotland.
- Robert Tappan Morris: Created first computer worm released on the Internet. Now a CS professor at MIT.

Hacking Solution

<table>
<thead>
<tr>
<th>Hacker</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gary McKinnon</td>
<td>Case pending</td>
</tr>
<tr>
<td>Robert Morris</td>
<td>3 years probation / $10,000</td>
</tr>
<tr>
<td>Kevin Mitnick</td>
<td>5 Years in Prison</td>
</tr>
<tr>
<td>Kevin Poulsen</td>
<td>5 Years in Prison / $65,000</td>
</tr>
<tr>
<td>Vladimir Levin</td>
<td>3 year in Jail / $240,000</td>
</tr>
<tr>
<td>Adrian Lamo</td>
<td>6 months house arrest / $65,000</td>
</tr>
<tr>
<td>Jonathan James</td>
<td>6 months in Prison</td>
</tr>
</tbody>
</table>
Abuse of Authority

Users have access privileges granted but institutional policy restricts proper access

Motivation

- Public disclosure
- Power trip
- Identity theft
- Intellectual property theft
- Sale of private information
- Imprudent curiosity
Vulnerable Systems

- Have important or sensitive information
- Have a large number of records
- Have users with broad access authority
- Have many users of the system

Tax Records
Military Records
Police Records
Transaction Data
Medical Records
Intellectual Property
Internet Services
Personnel Records

IRoram Ventures terminated or sanctioned for inappropriate access (April 2009 – March 2010)

Internet Services

Google Engineer, David Barksdale, was fired in July of 2010 after accessing call logs of a 15-year-old acquaintance to find details about his girlfriend, then threatening to call her.
Law Enforcement Records

Massachusetts, May, 2009. An audit of the state database of criminal records uncovered hundreds of queries about celebrities, including Brady, by personnel with no apparent work-related justification.

Transaction Data

Summer, 2010: an employee with Match Hospitality, the official ticket provider for FIFA, sold at least 250,000 records to black market ticket dealers. The records included the name, passport, and ticket information of customers who purchased tickets. The records sold for as much as 2.5 euros each.
November, 2007: Gary Min, a research scientist at DuPont was fined $44,500 for illegally accessing and downloading confidential documents worth almost $400,000 million.

SIPRNet
The “Private Internet” of the Department of Defense
More than half a million users all with broad, unrestricted access.
Private Bradley Manning

Leaked hundreds of thousands of classified documents to WikiLeaks

Manning’s 2010 Arrest

May 21: Manning confessed to former hacker Adrian Lamo in an AOL chat room.
May 23: Lamo met with FBI and Army officers and shows chat logs.
May 26: Manning Arrested in Iraq.

If Manning had not confessed, would his involvement been known?
James Clapper

Speaking on the Bradley Manning leak:

“But in the end, our system is based on personal trust. We had an egregious violation of personal trust in this case. We’ve had them before. We’ll have them again.”

National Intelligence Director

Medical Records

“There are just thousands of people who have access—and need to have access—to confidential information, and to try to change their behavior is a challenge”

Donald Bradfield
Johns Hopkins Health System
Palisades Medical Center  
New Jersey

After a motorcycle accident, more than two dozen employees illegally accessed Clooney’s medical records and those of his girlfriend, Sarah Larson.
California Health Privacy Law

In 2008:
• SB 541 Set health facility fines for breaches of privacy
• AB 211 Holds healthcare providers accountable for ensuring the privacy of patients

2009-2010 Fines

<table>
<thead>
<tr>
<th>Hospital</th>
<th>Fine</th>
<th>Patient Records</th>
<th>Employees Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bellflower</td>
<td>$437,500</td>
<td>1</td>
<td>23</td>
</tr>
<tr>
<td>San Bernardino</td>
<td>$375,000</td>
<td>207</td>
<td>2</td>
</tr>
<tr>
<td>Chico</td>
<td>$130,000</td>
<td>33</td>
<td>4</td>
</tr>
<tr>
<td>Marysville</td>
<td>$100,000</td>
<td>23</td>
<td>17</td>
</tr>
<tr>
<td>UCLA</td>
<td>$95,000</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Bakersfield</td>
<td>$25,000</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Traditional Solution

To the problem of unauthorized data access by insiders or abuse of authority . . .

Principle of Least Privilege

“Every privileged user of the system should operate using the least amount of privilege necessary to complete the job.”

—Saltzer

Communications of the ACM, 1974
Problems with “Least Privilege”

- Impractical for many organizations to implement effectively
- Giving every employee the perfect level of access is problematic
- Must choose to over-entitle or to under-entitle

Problems of Over-Entitlement

- Undue exposure
- Tendency toward escalation
  - Access rights are rarely revoked
- Current estimates are that 50-90% of employees are over-entitled
Problems of Under-Entitlement

- Granting exceptions can be expensive and time consuming
- In health-care settings, can be deadly
- Can still lead to over-entitlement

Even if the principle of least privilege were to be implemented perfectly, it cannot prevent the abuse of properly-accessed data.

Implementing the principle of least privilege alone is insufficient
Punitive Measures

- Sanctions
- Termination
- Civil
- Criminal

Observation

We tend to treat abuse of authority as we treat abuse of power. However, there is a fundamental difference.
The implicit or explicit expectation that one may be called on to justify one's beliefs, feelings, and actions to others.

—Lerner and Tetlock

A new approach: Accountability

- The master gives each servant a stewardship.
- The master travels to a “far country.”
- After a “long time” the master returns and holds a reckoning
Old Russian Proverb

Доверяй, но проверяй.

Trust, but verify.

Accountability is not Surveillance

Big Brother

Jeremy Bentham 1790 Panopticon
Effects of Surveillance

- Increases rule compliance
- Decreases Employee Morale
- Increases dissatisfaction

Accountability Theory

With the increase in the perception that an individual’s identity is known or that his actions will be evaluated, the behavior of that individual will be more consistent with social norms.
Main Factors of Accountability

- Identifiability
  A person’s “knowledge that his outputs could be linked to him.”
  —Williams et al.
- Evaluation

Trick-or-treat Study
Evaluation

“Performance will be assessed by another according to some normative ground rules and with some implied consequences.”

—Lerner and Tetlock

Areas of application

• Psychology
• Organizational Behavior
• Marketing
• Management
Prior Accountability Findings

Increasing accountability leads to:

• Reduced norm-breaking behavior
• Reduced risk-taking behavior
• Increased job performance

Accountability Theory is not Deterrence Theory
Deterrence Theory

Increasing the severity, certainty, or clarity of the consequences of an activity reduces the likelihood that an individual will engage in the activity.

Prop. 1: Increasing the perception of identifiability reduces rule violation behavior

Empirical Study:

Prop. 2: Increasing the perception of the likelihood of evaluation reduces rule violation behavior
Experimental Setting

- Introduction to Java Programming
- Online-homework submission system
- 84 Students
- One semester

Homework Submission System for
CS 142, Fall 2010

http://homework.byu.edu

Username: student200
Password: cb6pwqtt

For system questions, contact
Professor Vance: Anthony@vance.name
Measurement

Rule Violation Frequency:
Each rule violation counts

Rule Violation Instances:
Rule violations are collapsed to the assignment level

Hypotheses

Control
Expect No Difference

Experimental Groups
Identity Reduces Violations
ID & Log Reduces Violations

Treatment
Identity Reduces Violations
Log Reduces Violations

Expect No Difference
### Between Subjects Results

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>P value</th>
<th>Direction as expected?</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1a: Instances of access policy violations will be less in the high identifiability condition than in the low.</td>
<td>0.016</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>H1b: Frequency of access policy violations will be less in the high identifiability condition than in the low.</td>
<td>0.067</td>
<td>Yes</td>
<td>Yes*</td>
</tr>
<tr>
<td>H2a: Instances of access policy violations will be less in the high evaluation condition than in the low.</td>
<td>0.027</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>H2b: Frequency of access policy violations will be less in the high evaluation condition than in the low.</td>
<td>0.022</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Within Subjects Results

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>P value</th>
<th>Direction as expected?</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1c: Instances of access policy violations will be less in the high identifiability condition than in the low.</td>
<td>0.018</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>H1d: Frequency of access policy violations will be less in the high identifiability condition than in the low.</td>
<td>0.025</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>H2c: Instances of access policy violations will be less in the high evaluation condition than in the low.</td>
<td>0.023</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>H2d: Frequency of access policy violations will be less in the high evaluation condition than in the low.</td>
<td>0.115</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Behavior as Predicted
Peeking (Overall)

Capitalization Behavior
Peeking (Overall)
What accounts for the increase of rule violation behavior in the last period?
Implications of Research

- Increasing perception of accountability affects user behavior
- Increasing the perception of identifiability reduces rule-breaking behavior
- Increasing perception of the likelihood of evaluation has a mixed effect
Future Research

Ongoing

User Types
Are there different types of people who behave differently under different conditions of accountability, as we saw in the last experimental period?
Can these user type be predicted?
Analysis of User Behavior in Control Group

Saints
Gradual Descent

Recreants
Other Research Topics

- Effect of rolling log vs. static log
- Effect of log in isolation
- Manipulation of the likelihood of an audit
- Effect of making log public
- Effect of showing log to information owner
- Effect of random photograph
- Effect of biometric logging
An altogether too brief

History of Hacking

Gary McKinnon

McKinnon is Scottish systems administrator accused of the biggest military computer hacking exercise of all times by the US government.

McKinnon is also accused of copying data, account files and passwords into his own computer.

US authorities pegged the cost of tracking and rectifying the problems caused by his hacking at over $700,000.
Robert Tappan Morris

Morris is an American computer scientist, known for creating the first computer worm on the Internet called the Morris Worm in 1988.

He became the first person convicted under the Computer Fraud and Abuse Act.

He is a professor in the department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology.

Kevin Mitnick

Mitnick started out exploiting the Los Angeles bus punch card system to get free rides. He also dabbled in phone phreaking. Although there were numerous offenses, Mitnick was ultimately convicted for breaking into the Digital Equipment Corporation’s computer network and stealing software.

He is now a computer security consultant, author and speaker.
Kevin Poulson

Also known as Dark Dante, Poulsen gained recognition for his hack of LA radio's KIIS-FM phone lines, which earned him a brand new Porsche, among other items.

Authorities began to pursue Poulsen after he hacked into a federal investigation database. During this pursuit, he further drew the ire of the FBI by hacking into federal computers for wiretap information.

Jonathan James

Also known as "c0mrade," James gained notoriety when he became the first juvenile to be sent to prison for hacking. He was sentenced at 16 years old.

James's major intrusions targeted high-profile organizations. He installed a backdoor into a Defense Threat Reduction Agency server. James also cracked into NASA computers, stealing software. James said, "The code itself was crappy . . . certainly not worth $1.7 million like they claimed."
Adrian Lamo

Lamo's claim to fame is his break-ins at major organizations like The New York Times and Microsoft. Dubbed the "homeless hacker," he used Internet connections at Kinko's, coffee shops and libraries to do his intrusions.

Lamo's intrusions consisted mainly of penetration testing, in which he found flaws in security, exploited them and then informed companies of their shortcomings. His hits include Yahoo!, Bank of America, Citigroup and Cingular.

Vladimir Levin

Vladimir Levin led a Russian hacker group in the first publicly revealed international bank robbery over a network.

Levin used a laptop computer in London, England, to access the Citibank network, and then obtained a list of customer codes and passwords. Then he logged on 18 times over a period of weeks and transferred $3.7 million through wire transfers to accounts his group controlled in the United States, Finland, the Netherlands, Germany, and Israel.
Caption:

Title