

INTO THE BREACH: SECURITY BREACHES AND IDENTITY THEFT

Introduction

The public is growing more concerned as a number of security breaches involving high profile organizations have recently been widely publicized in the media. Although security breaches have been occurring for many years, public knowledge of their existence also has increased because many state laws require that individuals whose sensitive personal information is exposed be notified of the breach.¹

Security breaches put individuals at risk for identity theft. A security breach occurs when there is unauthorized acquisition of, or access to, records containing the sensitive personal information of an individual. Sensitive personal information can include a person's name and address in combination with a Social Security number, his or her date of birth, financial account information, driver's license number, medical information, or biometric data.²

AARP has examined a number of publicly disclosed security breaches to establish what kinds or organizations are being breached and the cause of the breaches. Based on our analysis, it is possible to distinguish some trends.

Methodology

The breaches analyzed in this report have been identified from a compilation of

¹ Currently 33 states have laws requiring public disclosure of security breaches containing sensitive personal information. (For a list of state breach laws, see <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>.)

² Biometric data identify a person through the measurement of a physical feature or repeatable action (for example, fingerprints, DNA sequence, hand written signature, or voice print).

publicly disclosed security breaches maintained by the Identity Theft Resource Center (ITRC).³ A total of 244 breaches dating from January 1, 2005 through May 26, 2006, potentially exposing the names of 89.8 million persons, are included in the analysis.⁴ This list identifies the entity suffering the breach, the number of potential individuals exposed by the breach, and the cause of the breach.

Based on ITRC information, entities reporting breaches were placed into one of the following categories:

- Educational institutions: includes all levels of public and private educational facilities including colleges, universities, and affiliated entities (such as alumni organizations).
- Healthcare organizations: includes hospitals, healthcare services, and healthcare insurers.⁵
- Financial services companies: includes banks, insurance companies, and investment services.
- General businesses: includes businesses not related to any of the other categories.
- Government agencies: includes federal, state, and local government agencies.

³ The Identity Theft Resource Center (ITRC) is a nonprofit organization that provides consumer and victim support and advises governmental agencies, legislators, and companies about identity theft crimes.

⁴ The list (available at <http://www.idtheftcenter.org/breaches.pdf>) was last updated on June 14, 2006 and was accessed for the purposes of this report on June 19, 2006.

⁵ Breaches at healthcare facilities associated with educational institutions are included in this category rather than under the education category.

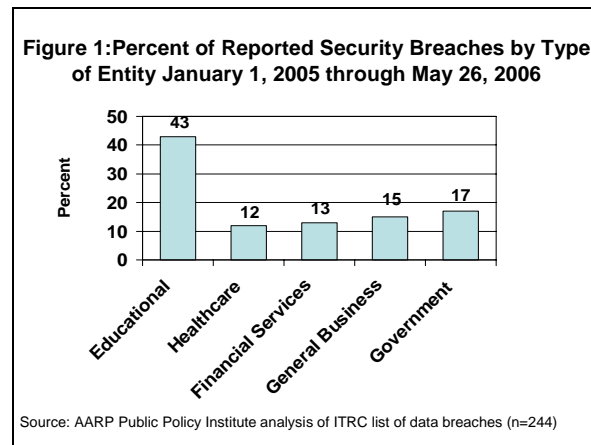
The reported breaches were then categorized by the cause of the breach:

- Hacker: illegal access through the Internet to data contained in a computer system by a person(s) external to the breached entity.
- Physical theft: the theft of computers, computer equipment (including computer data storage media), or paper files.
- Improper display: allowing sensitive personal information to be viewed by those who should not have access (for example, printing of Social Security numbers on address labels, inadvertently making sensitive personal information accessible on Internet sites that can be viewed by the general public, or not properly disposing of files containing sensitive personal information).
- Insider access: an employee or contractor stealing or providing others with access to sensitive personal information held by his or her employer.
- Lost backup: data storage media containing sensitive personal information lost in the process of transferring the media to another location.
- Not specified: the specific cause of the breach was not publicly disclosed by the entity suffering the breach.

Security breaches resulting from hackers and insider access have the potential to be the most damaging as these breaches are the result of a deliberate attempt to gain access to sensitive personal information. For other types of breaches, it is often not immediately apparent whether sensitive personal information was acquired by, or passed on to, those seeking to commit identity theft, but this outcome cannot be ruled out.

Findings

The analysis finds that educational institutions are more likely than any other type of entity to report having had a security breach. In fact, educational institutions were more than twice as likely to report suffering a breach as any other type of entity, while government agencies and general businesses were the next most common type of entity to report a breach (Figure 1).



An examination of the most frequent cause of reported security breaches reveals that a third (33 percent) of all breaches were caused by hackers who broke into computer systems to gain access to sensitive personal information (Figure 2).

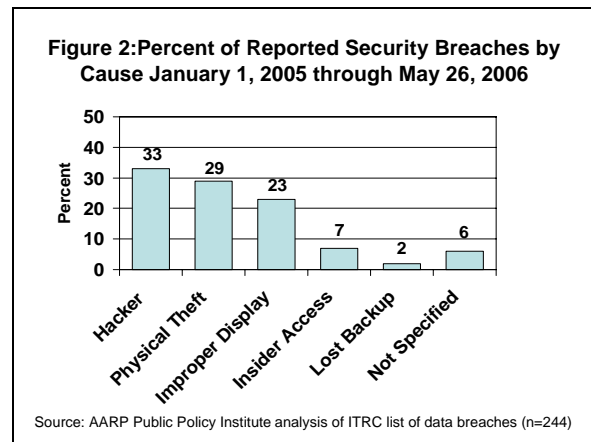


Table 1: Number of Reported Security Breaches by Type of Entity and Cause of Breach, January 1, 2005 through May 26, 2006

	Educational	Healthcare	Financial Services	General Business	Government	Total
Hacker	55	2	5	12	7	81
Physical Theft	14	20	14	11	12	71
Improper Display	26	3	2	7	17	55
Insider Access	2	4	5	2	3	16
Lost Backup	0	0	5	1	0	6
Not Specified	7	0	2	3	3	15
Total	104	29	33	36	42	244

Source: AARP Public Policy Institute analysis of ITRC list of data breaches, 2006.

Table 2: Number of Potential Victims* of Security Breaches by Type of Entity and Cause of Breach, January 1, 2005 through May 26, 2006

	Educational	Healthcare	Financial Services	General Business	Government	Total
Hacker	1,849,079	74,000	40,181,000	2,038,900	670,118	44,813,097
Physical Theft	1,503,743	898,450	756,500	598,523	26,867,330	30,624,546
Improper Display	94,791	3,623	0	398,500	2,124,734	2,621,648
Insider Access	106,003	27,140	681,863	206,100	4,515,000	5,536,106
Lost Backup	0	0	5,390,000	600,000	0	5,990,000
Not Specified	60,500	0	6,000	180,874	9,500	256,874
Total	3,614,116	1,003,213	47,015,363	4,022,897	34,186,682	89,842,271

* The number of potential victims was not disclosed in 35 of the reported breaches.

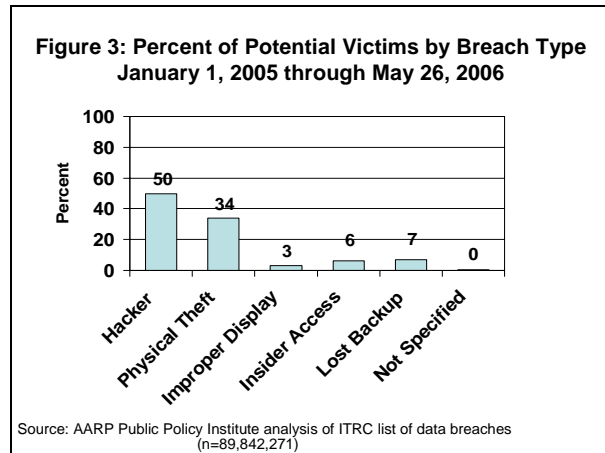
Source: AARP Public Policy Institute analysis of ITRC list of data breaches, 2006.

Physical theft of computers, computer equipment, or paper files is the next most common cause of security breaches, followed by improper display.

Table 1 shows the number of reported security breaches by the type of entity and cause of the breach. For educational institutions and general businesses, hackers are the most common cause of a security breach. Healthcare and financial services entities are more likely to report suffering a breach due to the physical theft of computers, computer equipment, or paper files, while government agencies are most likely to report suffering a breach as a result of the improper display of sensitive personal information.

Table 2 shows the number of persons who are at risk of identity theft as a result of security breaches by the type of entity and cause of breach. For educational institutions, financial service entities, and general business entities, security breaches by hackers created the largest number of potential victims. At healthcare entities and government agencies, the physical theft of computers, computer equipment, or paper files created the largest number of potential victims.

Overall, security breaches caused by hackers exposed the greatest number of individuals to potential identity theft, followed by the physical theft of computers, computer equipment, or paper files (Figure 3).



Summary and Implications

This analysis finds that 40 percent of the publicly disclosed security breach incidents were caused by hackers or insider access specifically targeting sensitive personal information. Breaches caused by hackers or insider access put the sensitive personal information of 50 million individuals (making up 56 percent of all breach victims) at risk of identity theft.

Because security breaches can pose a substantial risk of identity theft to those whose sensitive personal information is exposed, it is critical that these individuals be notified when breaches occur. This provides an opportunity for individuals put at risk by the breaches to take appropriate action to reduce the chances of harm should identity theft occur.

*Written by Neal G. Walters
AARP Public Policy Institute
601 E St., NW
Washington, DC 20049
202-434-3910; E-Mail ppi@aarp.org
July, 2006
© 2006 AARP <http://www.aarp.org/ppi>
Reprinting with permission only*