How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management

Divakaran Liginlal, Inkook Sim, Lara Khansa

Article history:
Received 7 May 2008
Received in revised form 25 September 2008
Accepted 26 November 2008

Keywords:
Privacy
Slips
Mistakes
Regulatory compliance
Information activity
Privacy controls

ABSTRACT
Privacy breaches and their regulatory implications have attracted corporate attention in recent times. An often overlooked cause of privacy breaches is human error. In this study, we first apply a model based on the widely accepted GEMS error typology to analyze publicly reported privacy breach incidents within the U.S. Then, based on an examination of the causes of the reported privacy breach incidents, we propose a defense-in-depth solution strategy founded on error avoidance, error interception, and error correction. Finally, we illustrate the application of the proposed strategy to managing human error in the case of the two leading causes of privacy breach incidents. This study finds that mistakes in the information processing stage constitute the most cases of human error-related privacy breach incidents, clearly highlighting the need for effective policies and their enforcement in organizations.

1. Introduction
Information privacy has recently attracted increased corporate attention. Privacy breach incidents not only result in loss of customer goodwill and trust; but they also have serious regulatory implications. Many U.S. firms are forced by privacy laws to report privacy breach incidents, resulting in negative publicity and heightened public awareness. Therefore, corporate decision-makers are instituting measures to prevent or mitigate the adverse effects of privacy breaches.

Human error, as a cause of data breaches, has received very little attention from researchers. Wood and Banks (1993) judged human error as the most frequent cause of data breaches in the organizations studied. Lewis (2003) also concluded that human error accounts for about 65% of data breach incidents resulting in economic loss. Schultz (2005) argued that information security is primarily a people problem – since technology is designed and managed by people, leaving opportunities for human error. Otto et al. (2007) pointed out that an important measure put in place by Choice Point after their infamous data breach incident is aimed at addressing the problem of high error rates in customer records. The authors emphasized the need for companies collecting and selling personal information to build a low-cost means of eliminating harmful errors from customer records. However, with emphasis primarily given to technical safeguards, firms routinely overlook human error as a major cause of privacy breaches. Human error arises from human–machine interface issues, work environments that stress workers, and other situational components. Besides bringing out the significance
of human error as an important cause of privacy breaches, this paper aims to systematically analyze these underlying issues from both an organizational and a systems perspective and come up with a comprehensive error management strategy.

1.1. Information privacy and the regulatory imperative

Defining the term ‘privacy’ is a difficult task as the associated semantics differ from person to person and culture to culture, aside from being context dependent. Individuals are willing to sacrifice privacy for rewards, usability, or other factors. Privacy is often related to the notions of anonymity, security, control, and access (Altman, 1975). Westin (1967) asserted that the right for privacy includes some degree of control over personal information that others collect and transmit, and embodies a right to verify the accuracy of this information. The author identified four privacy states: solitude, intimacy, anonymity, and reserve and five privacy functions: personal autonomy, emotional release, self-evaluation, and limited and protected communication. Culnan (2000) defined privacy as “people’s ability to control the terms under which their personal information is acquired and used.” Boyle (2003) attempted to reconcile these classical definitions with recent technological developments and experiences in the ubiquitous computing area. The author examined three elements of privacy: (i) solitude, or control over one’s personal interactions with other people; (ii) confidentiality, or control over other people’s access to personal information; and (iii) autonomy, or control over what one does. Turr (1985) defined privacy as “the right of individuals to control the process of collection, storage, processing, dissemination, and use of their personal information.” In the information systems literature, Smith et al. (1996) a frequently cited empirical study of individuals’ concerns about organizational use of personal information. The authors defined four factors (collection, secondary use, error, and improper access) which determine the construct ‘concern for information privacy’ (CFIP). As is evident from this literature survey, control has emerged as a key concept in understanding information privacy.

With the rapid growth of the Internet and mobile technologies and the enhanced risk of privacy breaches, the issue of privacy has received a lot of attention from lawmakers. Appendix A lists important privacy regulations and summarizes privacy-related requirements that organizations need to comply with. Apart from these listed regulations, new federal privacy legislation has been proposed to address the pervasive issue of identity theft. The specific provisions in the proposed legislation address issues such as the individual’s ability to access and correct personal electronic information, different types of security controls for safeguarding against privacy breaches, the institution of a proactive security program by organizations, and the imposition of severe penalties if privacy breaches occur.

1.2. Research questions and organization of the paper

We address the following research questions in this paper:

1. Is human error a significant cause of privacy breaches in U.S. firms?
2. What are the primary causes of human errors leading to privacy breaches?
3. How do organizations effectively address the problem of human error leading to privacy breaches?

The rest of the paper is organized as follows. In Section 2, we develop a model to categorize the different types of human errors across different information activities in the organizational workflow and present an illustrative example of the model’s application. Section 3 presents our analysis of publicly reported privacy breach incidents in the U.S. to show the significance and impact of human error in organizations. In Section 4, based on a content analysis of the privacy breach incident reports and a review of the extant literature, we identify the major causes of human error that results in privacy breaches. We then develop and illustrate a defense-in-depth solution strategy for organizations to address human errors that lead to privacy breaches. Finally, we summarize the contributions and limitations of our work along with a description of ongoing related research.

2. Human error and privacy

2.1. Modeling human error

Reason (1990) defined error as “the failure to achieve the intended outcome in a planned sequence of mental or physical activities when failure is not due to chance.” The author proposed a generic error modeling system (GEMS), which categorizes errors into slips and mistakes. Slips describe the incorrect execution of a correct action sequence and mistakes refer to correct execution of an incorrect action sequence. Mistakes represent the situation where a person makes a wrong decision but executes it correctly. Reason termed mistakes as “planning failures” and slips as “execution failures.” The term ‘mistake’ can be interpreted as the result of an intentional act involving faulty conceptual knowledge, incomplete knowledge, or incorrect action specification. On the other hand, a malicious act is also intentional but is directed at causing harm.

Human error is cited as a significant cause of accidents in several domains. For instance, medical error is reportedly the eighth leading cause of death in the U.S. (Dekker, 2007). The decentralized and fragmented nature of the health care delivery system and the resulting lack of communication and coordination of care among multiple providers lead to most medical errors (Dekker, 2007). In the aviation industry, three-quarters of all air carrier accidents are attributed to operator mistakes (Shappell et al., 2007). In online banking, security threats reportedly have more to do with human error and the usability of systems than any other issue (Kjaerland, 2006). Stanton et al. (2005) have also analyzed end user security behaviors. Their national survey of computer end users determined that naive mistakes, such as poor password hygiene, constituted the largest category of low expertise behavior with a significant impact on information security. Kraemer and Carayon (2007) built a framework that classifies different types of human errors and identifies specific human and organizational factors contributing to computer and
information security. However, none of the studies related to information security offered a comprehensive framework aimed at mitigating the effects of human error.

The GEMS taxonomy is useful since it provides a simple way of capturing most manifestations of human error and also facilitates the search for methods of error correction. In his study of the taxonomy of privacy, Solove (2006) identified three inter-related information activities in organizational workflows encompassing the collection, processing, and dissemination of information. Our model of human error combines the two approaches by applying the GEMS taxonomy across these three information activities.

2.2 Applying the human error model to loan processing

Fig. 1 depicts the information flow associated with loan processing in a bank following the schemas used in Antón et al. (2004). In the illustration, the term ‘personally identifiable information’ (PII) denotes any piece of information which can potentially be used to uniquely identify a customer.

The first step in loan processing involves the collection of personal information. In most cases, the loan officer interrogates the customer and runs a background check to acquire supporting information. An example of a mistake that could plausibly occur during this information collection activity is that of an overzealous loan officer attempting to acquire more private information than what is allowed in the company’s task manual. On the other hand, a slip might occur when the loan officer is distracted during data entry. Also, a slip or mistake may plausibly occur when, due to the exigencies of the work situation, the loan officer designates the task of entering the customer’s PII to a subordinate with a lesser skill set. During the information processing activity, the collected information is stored in a database and transferred internally or externally in raw, aggregated, or summarized form. Such information may be erroneously disclosed in a variety of ways during storage or transmission. For instance, the loan officer may discuss details of the loan application with the loan approval department in an open hall where the conversation is overheard by other people. Or, when notifying a customer of the acceptance status, the mailing clerk may use a wrong mailing address and reveal sensitive personal information to the wrong recipient. In the information dissemination stage, de-identified information about a customer may be disclosed to third parties for secondary use such as for market research. However, it is quite possible that the marketing department commits an error either by forgetting to de-identify or by failing to apply effective de-identification techniques.

Table 1 summarizes these illustrative loan processing scenarios involving privacy breach incidents, categorized according to our human error model.

3. The impact of human error on privacy: evidence from U.S. firms

A survey by Datamonitor (2007) determined that human error is the most frequent and significant cause of security incidents and data exposure in organizations. The Identity Theft Resource Center (ITRC) found that the data breach count for the first 6 months of 2008 shows an increase of 69% over the same period in 2007 and is at an all time high (Identity Theft Resource Center, 2008). Although human error and poor data handling policies and procedures continue to be significant in the 2008 data exposures, theft of data, either by external or internal sources, is the primary way information has been compromised. The Computing Technology Industry Association (Comp TIA) has consistently found since 2004 that human error is the main reason for security breaches. Their 2008 report (Computer Technology Industry Association, 2008) identified spyware, the lack of user awareness, and
virus and worm attacks as the main causes of security breaches. Verizon Business Security Solutions analyzed 500 data breach cases that occurred in the period 2004–2008 (Baker et al., 2008). Their “2008 data breach investigations report” attributed 62% of breaches to significant internal errors that either directly or indirectly contributed to a breach, most of which could have been avoided through effective internal controls.

From these studies, it is apparent that firms have given less attention to the reduction of human errors relative to the measures to safeguard against malicious attacks and insider threats. This motivates our study of human error as a major cause of privacy breaches in organizations.

3.1. Data collection

We compiled a database of privacy breach incidents reported in the U.S. from January 2005 to June 2008. First, we collected privacy breach incidents from the sites of leading privacy rights organizations such as Privacy Rights Clearinghouse (www.privacyrights.org) and attrition.org. These sites maintain comprehensive archives of privacy breach incidents compiled from a variety of sources, including voluntary reports by affected individuals and media sources along with external links to detailed reports of each incident. During the given time period from January 2005 to June 2008, we found 975 incidents reported at attrition.org and 972 incidents at Privacy Rights Clearinghouse. Not surprisingly, both sources shared many incidents and there were a few incidents reported from countries other than the U.S.A. We carefully removed duplicates and narrowed our study to incidents involving U.S. firms. The primary reasons for confining the research to data from U.S. firms were the lack of a well-documented source for collecting worldwide data and the major differences in privacy laws among countries, for instance the U.S. and the European Union (Sullivan, 2006). When external links were missing or the linked articles did not deliver enough detail, we searched for the reports of such incidents on the web. Next, we supplemented our search with data from prominent search engines such as Google using privacy-related keywords like “privacy breach,” “information security breach,” and “computer security.” Although this approach is not guaranteed to yield an exhaustive list of incidents, it is an effective way of confirming the comprehensiveness of our data sample. We also perused the news archives of New York Times, Washington Post, and Financial Times using keywords “security” and “privacy.” Both terms are often used synonymously; besides, security breaches are often associated with privacy breaches. We applied the same screening process to collect cases that were accurate, complete, and relevant to our study objectives. The search results from the search engines and media archives were individually validated for relevance and accuracy and subsequently merged with the original compilation.

We believe our data collection methodology of using well-established secondary data sources and cross-checking the data with other prominent public sources yielded a fairly representative collection of the most important privacy breach incidents in the U.S. during the stated time period. Our approach to data collection has been employed in various other studies of a similar nature (Erickson and Howard, 2007; Bagchi and Udo, 2003; Cavusoglu et al., 2004). There remains the possibility that several non-public organizations have chosen not to report certain privacy breach incidents. However, the recent surge of identity theft incidents and online vulnerabilities has attracted the attention of media and privacy activist groups besides exacerbating consumer concerns. It is now uncommon that an important privacy breach incident remains unnoticed or unreported by any of these sources.

3.2. Applying the human error model

Two researchers independently analyzed the compiled database of privacy incidents to determine the underlying cause of the incident and the stage of information activity in which the incident occurred. Hacking attacks or intentional violations of an organization’s privacy policies were regarded as malicious. When a human error created a vulnerability that was subsequently exploited for malicious purposes, the resulting incidents were classified as human error-related. The researchers further classified all human error incidents into those arising from either mistakes or slips. In general, the available descriptions of the breach incidents were of sufficient clarity to easily determine the cause of the incident, i.e., human error-related or intentional. The result was an observed inter-rater agreement of 0.94 with Kappa 0.84 (Z-statistic = 8.36;

<table>
<thead>
<tr>
<th>Slips</th>
<th>Mistakes</th>
<th>Information collection</th>
<th>Information processing</th>
<th>Information dissemination</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Data entry error</td>
<td>- Collecting information beyond requirement or unrelated to the purpose</td>
<td>- Leaving sensitive information accessible to others physically or electronically, such as losing a USB drive containing data</td>
<td>- Releasing PII to third party through wrong email address entry</td>
<td></td>
</tr>
<tr>
<td>- Incorrectly recording privacy policy agreement</td>
<td>- Insufficiently protecting stored information, e.g., forgetting to encrypt</td>
<td>- Releasing PII to an unauthorized party</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Unintentionally providing access to unauthorized individuals</td>
<td>- Storing or handling PII in unsecured manner for the sake of simplicity or efficiency</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Secondary use of information during processing</td>
<td>- Ensuring data is encrypted and protected</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
two-tailed $p$-value < 0.0001). However, the determination of whether a human error stemmed from a slip or a mistake was relatively more difficult. The observed inter-rater agreement in this case was 0.867 with Kappa 0.712 (Z-statistic = 6.12; two-tailed $p$-value < 0.0001). A third researcher served as an adjudicator to resolve conflicts and create the final data set used for trend analysis.

The following examples cover each of the six categories, i.e., slips and mistakes occurring in each of the three stages of information activities.

1. On January 1, 2005, a Foxtel spokeswoman told the Herald, “Due to human error the customer’s original opt-out request was not recorded. Foxtel regrets the mistake and acted to correct the error as soon as it was notified.” We categorize this act of wrongly executing action plans as a slip during information collection.

2. On January 9, 2006, the U.S. Homeland Security Department admitted that it collected more information than it had originally intended in its domestic airline passenger data scheme. Since the excessive data collection constituted a correct sequence of actions directed at achieving the wrong goal, we treat this and other similar cases as mistakes in information collection.

3. On June 2, 2006, personal information of Humana customers enrolled in the company’s Medicare prescription drug plans was compromised when an insurance company employee called up the data through a hotel computer and failed to subsequently delete the file. We categorize this incident as a slip in the information processing stage.

4. On February 6, 2007, the New York Department of Labor lost personal information when a laptop was stolen from a state tax auditor’s apartment. In fact, a great number of reported privacy breaches seem to stem from incidents of laptop thefts. In some cases, it is difficult to exactly ascertain whether a mistake or a slip resulted in loss of data. While the theft itself is beyond the victim’s control, the act of taking home a laptop containing sensitive information, especially without proper encryption and other safeguards, is, in general, a mistake. From a compliance perspective, organizations are required to have acceptable usage policies related to laptops (Datamonitor, 2007). Thus, if a laptop gets stolen either the concerned employee did not follow policies with regard to physically securing the laptop or the data itself existed in unencrypted form easily retrievable by the thief. In either case, we categorize the breach incident as a mistake during the information processing stage.

5. On January 1, 2007, the Wisconsin Tax Department mailed tax forms in which SSNs were inadvertently printed on the front of a few Form 1 booklets. We consider this incident as a slip in the information dissemination stage.

6. On March 1, 2006, the Ohio Secretary of State’s office posted SSNs, dates of birth, and other personal data of citizens on a state web site as part of a routine web posting. The lack of knowledge and understanding of privacy issues by the employee seem to have caused this breach. We categorize this incident as a mistake in the information dissemination stage.

3.3. Analysis

3.3.1. Results of trend analysis of all reported incidents

Of the 1046 total privacy breach incidents in our compilation, human error accounted for about 67% (701) of the incidents and malicious acts accounted for the remaining 33%. We studied the privacy breach incident trends over the period January 2005 to June 2008. Fig. 2 clearly demonstrates the consistent dominance of human error-related incidents over malicious incidents.

Next, we plotted the relative frequency of human errors, i.e., the ratio of human error to total incidents during the study period. In Fig. 3, human errors appear to be increasing at a decreasing rate. Our calculations show that the average ratio of human errors to total incidents over time is 64.12% with a standard deviation of 19.64%. The correlation coefficient (R-squared value of 58.64%) measures how good the fitted line meets the data. The highest variation around the mean occurs before March 2007. Since then, the overall trend in human errors relative to total incidents started decreasing with less variability. The ITRC report for 2008 (Identity Theft Resource Center, 2008) also confirmed this decreasing trend in human errors relative to other attacks, especially those involving theft of data.

Of the human error-related instances, 516 incidents occurred due to mistakes and 185 incidents resulted from slips. Further, 88% of the mistakes occurred during the information stage and 73% of slips occurred during the information dissemination stage. Fig. 4, which displays the trends in human error-related instances, shows that mistakes consistently outnumbered slips as a reported cause of privacy breaches during the period of the study.

3.3.2. Examining incident reports for public firms

Publicly-traded companies are compelled to report privacy breaches for three reasons. First, they are bound to act in the best interest of shareholders, including avoiding unnecessary litigations and excessively bad reputation caused by not taking responsive measures to a privacy breach. SEC and FTC regulations require publicly-traded firms to report to investors all privacy breach incidents that have a significant impact on the shareholders of the firm. Second, public firms are governed by specific legislation depending on their domains of interest. Finally, a majority of the states in the U.S. require that organizations notify the affected parties about a privacy breach incident. Appendix A discusses the legislation in greater detail.

Fig. 2 – Trends in privacy breach incidents for all firms.
In order to observe the effects of such regulations on privacy breaches, we focused on a subset of our sample that is solely composed of publicly-traded companies. We compiled a total of 181 privacy breach incidents targeted at public companies during the given time period. Fig. 5, which displays the trends of breach incidents in public firms, demonstrates that human errors have consistently outnumbered malicious attacks as a cause of privacy breaches. Comparing Fig. 5 with Fig. 2, which relates to the entire data set, we record a lower proportion of incidents due to malicious acts for public firms. This suggests that, relative to other organizations, public firms are more focused on ensuring better safeguards against malicious acts, while their efforts to mitigate human error-related incidents have been less effective.

To statistically identify any differences in the ratio of human errors to total errors among public and non-public target firms, we conducted a Wilcoxon Signed-Rank paired test using the ratios of human errors to total incidents, aggregated monthly. The sample size of 42 data points in the monthly time series encompassing incidents from January 2005 to June 2008 was sufficient to yield statistically significant results. The one-tailed test revealed that the ratio of human errors to overall incidents is, on average, higher for public firms compared to non-public firms (Z-statistic = 3.469; two-tailed p-value < 0.01). This high ratio of human error-induced incidents for public firms adds further evidence to our earlier observation that firms give more attention to safeguarding against malicious attacks. Further, this result is not surprising considering privacy breach incidents are likely to harm public firms more than private firms. The following section dissects the costs of such privacy breaches in general.

3.4. Analyzing the cost of privacy breaches

As companies grapple with the challenge of protecting their customer’s private data, research by the Ponemon Institute shows that the cost of failing to do is on the rise (Ponemon Institute, 2007). According to the study, data breach incidents...
cost companies $197 per compromised record in 2007, compared to $182 in 2006. Lost business opportunity, including losses associated with customer churn and acquisition, represented the most significant component of the cost increase. As identified below, the costs of privacy breaches extend beyond tangible losses and potential lawsuits by affected customers to loss of customer goodwill and in some cases collapse of the firm.

3.4.1. Tangible losses
These costs consist of physical data losses and equipment damage, as well as the man-hours required to recover from the breach. The Federal Trade Commission (FTC) not only penalizes breached firms but also mandates major improvements to prevent recurrence of such incidents. For instance, Choice Point was forced to pay U.S.$10 million in civil penalties and $5 million for consumer redress (Otto et al., 2007). The company also reached a separate settlement with 43 states over the breach.

3.4.2. Loss of market value
For public firms, the loss of market value reflects a decrease in investors’ confidence in the firm’s future economic prospects. Potential or actual monetary losses associated with security and privacy breaches have been shown in several event studies to stir a negative market reaction by stock market investors. The stock market’s reaction is often used as a measure of the potential economic impact of an event because investors are assumed to be rational and knowledgeable about the implications of this event. Campbell et al. (2003) recorded a 1.9% decrease in the market value of targeted firms following a security breach and a 5.4% market value loss when personal data were accessed. Cavusoglu et al. (2004) found a 2.1% loss in market value following breaches involving loss of confidential data. Similarly, Garg et al. (2003) found that the loss of credit card information had a higher negative market impact compared to the loss of other customer information. Acquisti et al. (2006) also confirmed such a negative market value impact (0.6% decrease).

To extend these prior results about the negative effect of privacy breaches to the 2005–2008 time span, we conducted an event study, using the market adjusted returns model as did Hendricks and Singhal (1996). Stock market data were gathered from the Center for Research in Security Prices (CRSP) database. We used Eq. (1) to obtain the abnormal returns associated with the various privacy breaches. The equation computes the abnormal return \( A_t \), for stock \( i \) at time \( t \), as the difference between the stock’s return at time \( t \) (\( R_{it} \)) and the market return (\( R_{mt} \)). We used the CRSP value-weighted index as the market return (\( R_{mt} \)).

\[
A_t = R_{it} - R_{mt}
\]

Similar to Gao and Iyer (2006), we chose an estimation window of 75 days. After screening out events with fewer than 75 days for estimation, we left with 151 events, spanning the period from January 2005 to June 2008. We used various evaluation windows ranging from 2 days prior to a particular event to capture any information leakage before public announcements, up to 9 days after the event to capture the impact of market momentum.

The results reveal a significantly negative mean cumulative abnormal return of 0.72% from 2 days before the breach to 1 day after the breach (t-statistic = −3.124) and a negative mean cumulative abnormal return of 0.59% from 2 days before the breach to 2 days after the breach (t-statistic = −2.974).

3.4.3. Damages for consumers
Consumers, whose private information has been stolen, could suffer from the risk of identity theft. About 30% of known identity thefts are estimated to be caused by corporate data breaches (Identity Theft Resource Center, 2008). Although, according to a U.S. Government Accountability Office (GAO) office report (U.S. Government Accountability Office, 2007), evidence directly linking the frequent breach incidents to resulting identity thefts is hard to determine, the monetary loss arising from identity theft, the countless obstacles to getting on with life, the resulting psychological dread, and offensive publication of illicitly acquired personal information are all aspects to be concerned about. The information obtained by insurance companies and employers could limit someone’s economic activities, or information obtained by government agencies could threaten one’s sense of autonomy and dignity (Cline, 2008). Although the U.S. courts have been reluctant to award tangible dollars for these intangible harms, customer lawsuits, if successful, can translate into monetary burdens in the amount of billions of dollars on the breached firm.

4. A framework for human error analysis and reduction of privacy breaches

Given the staggering costs of privacy breaches, a majority of them arising from human error, we first review methods proposed by researchers to address the problem of human error in general and data breaches in particular. Then, based on a literature review and an analysis of the compiled privacy breach incidents, we propose a defense-in-depth strategy to mitigate the effects of human error.

4.1. Literature review

Johnson and Goetz (2007) recommended five imperatives, when building security into organizations: change in focus from technology to behavioral issues, attention to the needs and demands of customers and business partners in relation to enhanced security, linking security metrics to business decisions, a proactive approach to security investments, and building a security culture through focused education. Trope et al. (2007), in their study of data governance practices, emphasized the need for greater attention to legislative requirements, due diligence in transactions and business alliances, and coherent information management strategies. Kark (2008) identified eight best practices for CISOs to devise a plan against information security breaches. A layered defense approach incorporating both the technology layer and the people and processes layer is a key ingredient. Kark’s other recommendations included the following: establish and test processes, build external
relationships, publicly acknowledge a breach as soon as the facts are verified, understand legal and jurisdictional requirements up front, empower the team to make decisions, conduct root cause analysis (Wilson et al., 1993), and continuously measure security policy compliance levels. Root cause analysis is an established methodology in various fields to identify why things went wrong and how to correct them. This retrospective approach to error analysis has its foundations in industrial psychology and human factors engineering. Reason (1990) also categorized error into: (i) active error, which generally occurs at the point of human interface with a complex system and (ii) latent error, which represents failures of system design. Root cause analysis is generally employed to uncover latent errors underlying an event.

Sanders and McCormick (1993) suggested training, selection, and design approaches as general strategies for error reduction. Mason (1992) used the GEMS error typology to come up with error reduction strategies. Accordingly, slips and lapses can be effectively addressed by design improvements and training. Mistakes can, in general, be addressed through training, clear labeling and color coding and techniques for redundancy. An increasing number of studies emphasized the impact of mistakes in organizations (Baker et al., 2008). Mistakes occur when there are planning errors or decision-making errors. In dynamic and complex environment settings, users are required to maintain high level of awareness and understanding of situation in addition to knowledge and skills to avoid such errors. Mistakes in most cases arise from incorrect or incomplete knowledge, misuse of knowledge, application of faulty heuristics, and information overload. These can be addressed through better education, decision support, information reduction, and enhancements to supervisory controls. Lourens (1989) recommended five steps for managers to implement an error management strategy: (i) create a database of past errors; (ii) reassess operator performance regularly; (iii) study operator habits during routine activity; (iv) use properly designed displays; and (v) make individuals aware of risk-enhancing factors in interactive work.

Applying GEMS to discern the influence of errors needs particular care. For instance, in the information collection stage, either a slip or a mistake could plausibly result in creating a wrong privacy policy agreement data record. The solution strategies differ in each case. Often with computers and other gadgets, user interface design with particular emphasis on display design and other usability considerations will go a long way in reducing mistakes. A lack of situation awareness (Endsley, 1995) has often been cited as one of the main causes of slips. Situation awareness is defined as “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.” Lack of activation, i.e., a momentary failure to apply the correct rule, cross talk, and perceptual confusion, are other main causes of slips. Better training, reducing interruptions and multitasking, and providing memory aids are very common methods for reducing slips. In their analysis of aviation accidents caused by pilot errors, Dismukes et al. (2007) argued that accidents can be understood only in the context of how the overall system operates. User interface design, along with workload and other environmental factors requires careful consideration. In fact, research into enhanced situation awareness emphasized the role of individual elements, environmental elements, and the interactions between the two in reducing operator error in various application domains (Endsley, 1995). Also, empirical evidence pointed to the need for addressing human errors differently in different situations depending on their cause, type, and environmental settings. Bratus et al. (2008) proposed that a user’s environment be separated into private, work, and public zones. Each action, such as saving a document or starting a program, would involve placing an actor, represented by an appropriate icon, into one of these zones. Actor icons would reflect the presence of executable or other active content, and the actor’s known and claimed origin. The objective is to evoke user intuitions connected to granting real world parties access to their private or work-related data with varying degrees of privacy and to checking these parties’ identity claims. Maxion and Reeder (2005) studied the causes of user error in user interfaces in general and in the case of file permissions in particular. The authors proposed a design method that can be applied to new generations of user interfaces so that the same user errors are not encountered over and over again in future user interfaces.

Drawing from these studies, we propose an error management program consisting of three steps: (i) conduct root cause analysis of all privacy breach incidents; (ii) institute a defense-in-depth strategy involving error avoidance, error interception, and error correction; and (iii) periodically evaluate the effectiveness of the operational and technical measures in place.

4.2. Categorizing privacy breach incidents

The case of human error has, in general, received very little attention in the context of information security. Kjaerland’s (2006) taxonomy of computer security incidents in commercial and government sectors only emphasized intentional attacks. The IT Compliance Institute reports the results of a survey conducted in 2007, which lists eight frequent causes of privacy breaches (IT Compliance Institute, 2007). The top three dominant causes of privacy breaches in 2007 were lost computer equipment, Internet threats, attacks, or hacks, and inappropriate skills associated with using information technology. We examined the privacy breach incident data set to determine the source of human error, i.e., whether or not information technology was involved, and the cause of the breach. The resulting taxonomy, shown in Table 2, confirms the findings of the IT Compliance Institute’s survey.

4.3. A defense-in-depth error management strategy and solutions to manage privacy breaches

Our analysis of the publicly reported privacy breach incident reports resulted in categorizing the sources of human errors based on process type (IT-enabled or manual) and data representation (electronic or non-electronic). As shown
in Table 3, for each combination of these categories, we consider three strategies: error avoidance, error interception, and error correction. The first strategy is meant to prevent human errors from occurring or at least reducing their frequency of occurrence. The second strategy aims at detecting the error and stopping it before damages occur, while the last strategy is intended at handling errors that have already occurred and providing some form of reversibility. The ultimate objective of designing error-resilient systems is to incorporate all three categories, thereby providing a defense-in-depth strategy. Although not discussed here, these strategies may be further customized based on the context of occurrence, i.e., organizational, team, or individual and the nature of error, i.e., cognitive or behavioral.

4.3.1. Error avoidance
In IT-enabled processes, errors are most often linked to a mismatch between the worker’s mental model of the system and the system’s actual state. Poor feedback and lack of experience are often two major causes of such mental model mismatches. The frequent training of users to enhance both their knowledge and skill is crucial for error avoidance under all circumstances. Training must focus on both concepts and procedures and evolve with the system to ensure that the developed mental models are sustained and kept current. Training programs need to be profound, recurrent, and designed to force operators out of their comfort zones. It is also desirable to have such recurrent training integrated into a system’s normal operation. Similarly, user interface design plays a significant role in avoiding errors involving the use of technology. For instance, wizards can guide a user through predefined tasks assuming that operators do not bypass them for expediency.

In recent years, considerable work has been done in the area of privacy-enhancing technologies (PET). Whenever information is handled electronically, an information space (Jiang and Landay, 2002) provides a way to organize information, resources, and services around important privacy-relevant contextual factors. The boundaries of such information spaces serve as a contextual trigger to enforce permissions that the space owners define. For instance, the demarcation of physical boundaries through location awareness and social- and activity-based boundaries through identity and activity awareness help implement privacy controls designed to avoid errors. In the case of non-electronic information, especially in medical settings, bar codes have traditionally been used to minimize errors (Ball et al., 2003). In non-IT-related instances, such as in the manual handling of paper records or spoken conversation, the use of memory aids to enhance situation awareness and automation helps avoid errors.

4.3.2. Error interception
Effectively designed and implemented technical and administrative controls serve as basic tools for intercepting errors. With IT-enabled processes, in which information is represented in electronic form, error interception is often achieved through the use of displays, monitoring, and privacy controls, such as buffering and alarms. For instance, when confidential emails are transmitted, a possible strategy to intercept errors is through buffering or queuing of the actual transmission. This provides a means of stopping the actual delivery of the message within a latency period during which an erroneously or rashly sent message can be recalled, discarded, or edited.

| Table 2 – Taxonomy of privacy breach incidents and their causes. |
|----------------------|----------------|----------------|
| Breach Type | Source of Error | Leading Cause of Breach |
| Human error | IT-enabled process: 600 (122) | 1. Lost computer equipment: 385 (99) |
| | Manual process: 101 (18) | 2. Inappropriate skill of using IT: 131 (14) |
| | | 3. Insufficient monitoring: 110 (15) |
| | | 4. Improper disposal of documents: 68 (11) |
| Malicious acts | IT-enabled process: 290 (36) | 5. User entry errors: 7 (1) |
| | Manual process: 55 (6) | 6. Internet threats, attack, or hack: 249 (29) |
| | | 7. Employee manipulation and malfeasance: 62 (10) |
| | | 8. Unauthorized access to IT: 34 (3) |

Note: Total number of incidents shown for each category (numbers in parentheses indicate those applicable to public firms).

| Table 3 – Strategies and solutions to manage privacy breaches due to human error. |
|----------------------|----------------|----------------|
| Source | Data representation | Strategies and solutions for error management |
| IT-enabled process | Electronic, e.g., transaction record | 1. Avoidance: Training, enhanced usability, and privacy control through context-aware systems |
| | Non-electronic, e.g., image printout | 2. Interception: Buffering, display design, monitoring, and alarms, and frequent audits |
| | | 3. Correction: Timely feedback, root cause analysis, overrides, and decision support systems |
| Manual process | Non-electronic, e.g., paper record, spoken conversation | 4. Avoidance: Training and usability-enhancement, bar codes |
| | | 5. Interception: Physical space control (RFID tags), induced delays, controls in workflow, and frequent audits |
| | | 6. Correction: Timely feedback, root cause analysis, and decision support systems |
| | | 7. Avoidance: Training, education, memory aids to enhance situation awareness (SA), and automation |
| | | 8. Interception: Manual controls in workflow, and frequent audits |
| | | 9. Correction: Timely feedback, root cause analysis, and decision aids |
The aforementioned techniques depend on the human ability to self-detect errors, since humans are prompt to detect errors immediately after their commission. The effectiveness of these techniques is also contingent upon the asynchronous nature of the related tasks, which allows for delay to provide recovery.

If information is in non-electronic form, error interception can be achieved through physical space control techniques (Ball et al., 2009), such as using RFID tags and through induced delays in the workflow. For instance, RFID tags attached to artifacts holding confidential information can be monitored to ensure that the protected information does not leave its designated physical boundaries. With manual processes, controls in the workflow such as a cross-verification by a second operator or authorization by a supervisor provide means of intercepting errors.

4.3.3. Error correction
A mechanism for timely error reporting is a prerequisite for error correction. This should be followed by root cause analysis in conjunction with the use of agile decision support for corrective actions. With electronic information, overrides may often be effective. An example is the ability to recall an email message or inhibit the display of its contents at the destination through the use of modified email protocols. One such implementation would involve the need to send a second message by the sender with a key to unlock the contents of the message. When the recipient attempts to read the original message, a callback function is triggered to request the key. From a compliance perspective, error tracking and logging systems are absolutely essential in organizations. Errors cannot be investigated and analyzed until they are identified. Most often, there will be insufficient information to remedy the error-inducing situations. A well-designed error reporting system will involve the documentation of errors, their timely investigation, and a well thought-out solution strategy rather than a blame game. It is crucial that a formal communication channel exists to self-detect errors, since humans are prompt to detect errors far in avoiding errors. It is necessary to monitor employees' use of PCs, computer networks and the Internet and to inform employees that monitoring will occur. The following are some useful error avoidance strategies: (1) classify information based on its sensitivity and assign security clearances to employees based on their data access needs; (2) introduce appropriate access controls for buildings and locations where computers are used; (3) periodically assess the vulnerability of computers and networks and of security devices such as alarms and locks; and (4) use CCTV and audio recording equipment to monitor buildings and areas where computers are in use. Finally, many organizations have an enforcement policy that warns employees of disciplinary action, up to and including termination of employment for violating acceptable use policy.

4.4. Applying the defense-in-depth strategy
We next examine how the proposed defense-in-depth strategy may be effectively employed to address the two primary causes, identified earlier, of privacy breach incidents due to human error.

4.4.1. Lost computer equipment
In almost all cases of lost computer equipment, human error plays a prominent role from the perspective of a privacy breach. Securing laptops can be accomplished using a variety of methods applied individually or in combination, such as the use of 'kill switches,' data encryption, and tracking. Encryption products have been largely used in government and financial institutions until recently but are now finding wider use with the advent of notification laws. Typical examples of human error involved in these incidents include misunderstanding or ignorance of organizational policies regarding computer use, failure to encrypt data, and poor monitoring.

4.4.1.1. Error avoidance. Many stolen computer equipment incidents arise from the lax application of physical safeguards by employees, such as misplacing or improperly securing equipment. This may be attributed to a lack of understanding of policies or overzealous actions in the interests of expediency and convenience. Frequently educating users about policies and properly training employees at all levels will go far in avoiding errors. It is necessary to monitor employees' use of PCs, computer networks and the Internet and to inform employees that monitoring will occur. The following are some useful error avoidance strategies: (1) classify information based on its sensitivity and assign security clearances to employees based on their data access needs; (2) introduce appropriate access controls for buildings and locations where computers are used; (3) periodically assess the vulnerability of computers and networks and of security devices such as alarms and locks; and (4) use CCTV and audio recording equipment to monitor buildings and areas where computers are in use. Finally, many organizations have an enforcement policy that warns employees of disciplinary action, up to and including termination of employment for violating acceptable use policy.

4.4.1.2. Error interception. Electronic marking techniques are useful in error interception. Alerting users when they access sensitive data is one useful technique. RFID-based physical tracking of equipment allows for the activation of alarm systems when such equipment leaves their allowed physical boundaries. Many organizations have started using software built into the BIOS that will automatically connect computers periodically to an online tracking service. This will help trace stolen laptops if the next user connects to the net (Computerworld, 2006). Firms should conduct regular property and equipment audits, record missing items, allocate responsibility for equipment to individuals, and establish measures to control use and movement of equipment.

4.4.1.3. Error correction. In many organizations, computers are required to first connect to an online service and regularly go through a checklist, noting things such as whether they have been booted up using legitimate access controls. If they have not, the service can launch procedures in order to inhibit the use of the machine. Kill switches such as those using remote obliteration of sensitive data also help to mitigate the impact on privacy. It is also important to have a good incident response plan and to make users aware of proper procedures in the event of a computer equipment loss. Timely reporting to both the organization's privacy officer and local law enforcement agency is critical. Further, it is important to determine the extent of the data loss by perusing backups and other records and ensure that passwords and encryption keys that facilitate access to the network are changed immediately.
4.4.2. Improper disposal of documents
It is absolutely essential for organizations to have policies and procedures governing the disposal of documents containing sensitive data such as social security numbers, and personal medical or financial information.

4.4.2.1. Error avoidance. User training is crucial to ensure competency with the procedures for document disposal. Marking sensitivity level clearly on documents helps enhance situation awareness. Also, placing more document shredders in easily accessible locations facilitates their increased use. Electronic documents should be flagged based on their level of importance. Deleting files through normal delete commands is not adequate. It is necessary to overwrite all relevant blocks of data within a file system multiple times before a file can be flagged as effectively deleted. This requires the use of special software. Similarly, it is necessary to ensure that unusable media be destroyed to avoid any possibility of information retrieval through dumpster diving.

4.4.2.2. Error interception. Warning banners or stickers on dump bins can potentially stop users from improperly disposing of documents. Adding one more control step in the disposal process and frequently auditing strengthen the monitoring process.

4.4.2.3. Error correction. Once error incidents are reported, they must be documented and investigated, with clearly spelled-out solution strategies to avoid future recurrence. Existing weaknesses in workflows and use of technology must be quickly addressed, and training procedures ought to quickly reflect these changes.

The other top three causes of human error are insufficient monitoring, inappropriate skill in using technology, and user entry errors. Error avoidance strategies in these cases need to focus on frequent and repeated training and education. Also, memory aids to enhance situation awareness will be helpful. Errors can be intercepted through the use of controls or checks in the workflow especially frequent auditing. Finally, a well-orchestrated strategy of tracking errors combined with root cause analysis facilitates the reduction of errors.

5. Conclusions and future work
Evident from our analysis, privacy breach incidents due to both slips and mistakes have been steadily increasing relative to malicious attacks, especially in public firms. Given the significance of these findings it is obvious that the management of human error should be of high priority in organizations. Since mistakes in the information processing stage constitute the highest percentage of errors, there is urgent need to enforce effective organizational policies. Our analysis empirically confirms the results of an IT Compliance Institute survey concerning the leading causes of breach incidents (IT Compliance Institute, 2007). Based on these results, we proposed a framework for managing human errors and minimizing the impact of privacy breaches.

Our study has several limitations. First, the results are based on secondary data sources, albeit in the form of a comprehensive and thorough compilation of reported incidents within the U.S. There exists the possibility that not all privacy breach incidents are reported publicly. Second, our analysis of the publicly reported incidents is limited by the depth of information available in each incident report. We therefore studied several recent reports that address the cause of privacy breaches in organizations. Due to these inherent limitations, generalization of our results must be done with caution. At the least, we argue that the study provides insight into a problem that has received very little attention from management and has not been delved into in prior literature. Further, we build a framework that managers, with limited time and resources, may use as a starting point to build strategies and solutions to prevent or mitigate the problem of human error.

Our study has several implications for managers. First, new systems and procedures are leading inducers of new types of error. Any new system or equipment should be evaluated for its potential impact on existing systems before installation. Second, procedural errors, especially in the information processing stage, require the most attention. Organizations must compulsorily develop clear and effective procedures to ensure that operators and supervisors are adequately trained to handle such errors. Future research is warranted in this area to identify procedures that may benefit from checklists or other user aids. Third, people tend to resist change and may be concerned about the risk for misuse of an error reporting system. It is important, when establishing such a system, that the focus be on the system or situation instead of the individual to blame. In order to identify and mitigate error-causing situations, organizations need to encourage accurate reporting as well as provide protection for the respondent. Finally, a major concern is the contribution of work-related fatigue to the commission of errors. This is a critical topic that needs attention by organizations to meet the standards mandated by regulations.

We have also undertaken a more detailed study to understand the underlying mechanisms and consequences of human error specifically related to compliance to the HIPAA privacy rule. Our research interests are divided into the following subsets: understanding the origin of human error, categorizing the types of errors resulting in HIPAA non-compliance by applying widely accepted models of human error, gauging the impacts of the errors, and developing techniques to manage human errors. Thus far, we have piloted a survey questionnaire which we plan to send out to about 250 HIPAA officers in the U.S. Subsequently, we plan to repeat the study in the financial sector to understand differences across these sectors. Our objective is to confirm the important finding in this paper that human error is the major cause of privacy breaches and to discern the kinds of errors and their cause and effects on organizations that are subject to key regulations such as HIPAA, GLBA, and FERPA.
## Appendix A.
Summary of key U.S. legislation with implications for information privacy

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Privacy focus</th>
<th>Specific provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>Specifies how protected health information (PHI) should be managed by covered entities.</td>
<td>• Organizations may only release PHI with the prior written consent of the individuals.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Organizations should take reasonable steps to ensure the confidentiality of PHI and maintain proper records.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Individuals maintain the right to request to retrieve their PHI and to correct any inaccurate information.</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act (GLBA)</td>
<td>Governs the collection and disclosure of customers’ personal financial information by financial institutions.</td>
<td>• Organizations must provide a consumer with a privacy notice when the consumer relationship is established and annually thereafter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The privacy notice must describe which information is collected, where and how that information is used, and how that information is protected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• It must identify the consumer’s right to opt-out of the sharing of information with unaffiliated parties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the privacy policy changes, the consumer’s consent must be obtained.</td>
</tr>
<tr>
<td>Family Educational Rights and Privacy Act (FERPA)</td>
<td>Regulates the rights and restrictions of parents, employees, and state agencies to access student educational records.</td>
<td>• Organizations must allow students to inspect and review their education records within 45 days of a request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Students maintain the right to request the amendment of their education records that they believe is inaccurate, misleading, or otherwise in violation of their privacy rights.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Schools must obtain the student or parent’s permission before allowing student records to be shared with a third party.</td>
</tr>
<tr>
<td>U.S.A. Patriot Act</td>
<td>Requires all U.S. businesses to provide access to customer information for law enforcement.</td>
<td>• Companies should establish a document management system to ensure ready access to documents and retention of documents relevant in litigation or other government investigation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Financial institutions must ensure they have procedures for identifying customer account information and the ability to verify customer identity and maintain records of information used to verify identity.</td>
</tr>
<tr>
<td>The Fair and Accurate Credit Transactions Act</td>
<td>Requires proper disposal of consumer report information and records.</td>
<td>• Any person or company who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.</td>
</tr>
</tbody>
</table>
Appendix A (continued)

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Privacy focus</th>
<th>Specific provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Identity Theft Penalty Enhancement Act</td>
<td>Establishes a new federal crime, i.e., aggravated identity theft.</td>
<td>• Any U.S. resident, knowingly transfers, possesses, or uses, without lawful authority a means of identification of another person or a false identification document will face punishment.</td>
</tr>
<tr>
<td>California SB 1386&quot; (See note about other state legislation)</td>
<td>Defines and specifies the notification requirements, procedures, and timelines of customers’ ‘personal information.’</td>
<td>• Specifies what type of data is subject to breach law (an individual’s name, social security number, identification card number, account or credit card number, date of birth, biometric data).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Any person or business who reasonably believes that personal information has been acquired by an unauthorized person is required to notify the affected party.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Notice must be provided to affected individuals using either written notice, electronic notice with customer’s consent, or a substitute notice.</td>
</tr>
</tbody>
</table>

California SB 1386 has influenced data breach legislation in most other states in the U.S.A. and is also a model for federal privacy legislation (see http://www.ncsl.org/programs/lis/privacy/idt-legis.htm).

REFERENCES


Cline J. When does a privacy breach cause harm? Computerworld; March 06, 2008.


Divakaran Liginlal (Lal) is an Assistant Professor of Computer and Information Sciences at the University of South Alabama. Lal received his BS in Communication Engineering from the University of Kerala, MS in Computer Science and Engineering from the Indian Institute of Science, and a Ph.D. in Information Systems from the University of Arizona. Before joining academics, he worked as a scientist for the Indian Space Research Organization (as a member of the Inertial Guidance System team for India’s Satellite Launch Vehicle program). His research has been published in journals such as the Communications of the ACM, European Journal of Operational Research, Fuzzy Sets and Systems, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Systems, Man, and Cybernetics, and Decision Support Systems. Lal has received funding support for his research and teaching from Microsoft Corporation, Hewlett Packard, CISCO, DOD at UW-Madison, and the ICAIR at the University of Florida. Contact him at diliginlal@cis.usouthal.edu.

Inkook Sim is a Ph.D. candidate in the Operations and Information Management Department at the University of Wisconsin–Madison School of Business. His research interests are in information privacy, social networking, context-aware system design, and IT productivity and evaluation. He holds an MBA from the University of Wisconsin–Madison and is a member of the Association for Information Systems and INFORMS. Contact him at isim@wisc.edu.

Lara Khansa is an Assistant Professor of Business Information Technology at Virginia Polytechnic Institute and State University. She received the Ph.D. in Information Systems, MBA in Finance and Investment Banking, and MS in Computer Engineering from the University of Wisconsin, Madison. Lara worked at GE Medical Systems as a software design engineer and earned the Green Belt Six Sigma certification. She has published in the European Journal of Operational Research and the Communications of the ACM. Her research interests are in the areas of business value of IT, economics of information security, and regulatory economics. She is a member of the Association for Information Systems, Institute of Electrical and Electronics Engineers, and Beta Gamma Sigma National Honor Society. Contact her at larak@vt.edu.