Blaming Noncompliance Is Too Convenient:

What Really Causes Information Breaches?

Karen Renaud | University of Glasgow

Little evidence exists that shows security policies reduce confidentiality breaches or information loss. However, organizations continue to put high demands on compliance to policy directives, sometimes creating impossible standards that employees feel interfere with their ability to work.

Information leaks can occur when outsiders breach organizations' systems or when insiders deliberately or inadvertently cause breaches. In 2009, the Computer Security Institute reported that the highest financial losses came from malicious insider attacks (60 percent of total losses).[1] This area merits investigation because, unlike with outsider risk, the situation shows no signs of improvement.

Employee behavior is challenging to manage. People endorse different personal standards of behavior, and you can't expect newcomers to know what constitutes acceptable behavior in a given organization. So, many organizations establish policies and procedures and provide training to make employees aware of them.

However, employees still occasionally cause information breaches. When a breach does occur, the subsequent investigation usually determines that the existing rules would have prevented the breach but weren't followed. The response is usually a review and tightening of processes, thereby making policy directives even more restrictive and prescriptive. The responsible employee is often disciplined and sometimes even dismissed.

Is this reasoning correct? Is the problem as simple as noncompliance? In considering this question, we must study the human element—the people who appear to be at fault. There might be good reasons for their "noncompliance." (For further information, see the "Why People Don't Comply" sidebar.)

To further investigate this problem, I conducted a study of employee adherence to the information security policies at one of the Scottish health boards of the UK National Health Service (NHS). I chose this type of organization because people are particularly sensitive about their health information being leaked, and it's vital to keep such information confidential.

Health Board Information Security Practices

The health board appeared to follow best practices in three areas.

Fostering a Security Culture

Employees must be aware of the contents of policies. Peter Drucker claimed that the organizational culture is a function of shared values.[2] It's clearly desirable to foster a shared value of confidentiality to minimize information breaches.

The health board had a range of training programs. Managers were required to ensure that all employees regularly attended training courses. Furthermore, the board disseminated new policies directly to employees' computers upon login. The employees had to indicate that they had read and understood the policy before they could access their computers.

Appointing Responsible Officers

Clive Vermeulen and Rossouw von Solms argued for three vital steps in fostering an information security culture in an organization.[3] The first is to appoint a security officer; the second and third relate to awareness and training.

1540-7993/12/$31.00 © 2012 IEEE

Why People Don't Comply

Elinor Madigan and her colleagues classified policy directive violations as errors of either omission or commission.[1] Omission errors occur when employees aren't sufficiently aware of policies.[2] If they're aware of the policies, the errors are presumably those of commission.

Gerald Cohen said that people don't obey known rules because either they can't or won't.[3] Sometimes an employee knows what's required but lacks the technical expertise to carry out the instructions, and therefore can't comply. For example, an employee could be required to password-protect files before emailing them but lack the expertise to do so.

Even if we assume that people are aware and able to comply, there are still other reasons why they don't. Peter Mascini posited that people disobey rules for three reasons:[4]

- the rules are a nuisance,
- they present an ethical dilemma, or
- they're impossible to follow.

The first category is clearly a *won't* situation and the last a *can't* situation (the middle one is harder to pigeonhole).

Even if employees can and do want to follow procedures, the reality is that people make mistakes, however well trained and well intentioned they might be. This could be due to cognitive limitations, task demands, the environment, or social and organizational factors.[5] Regarding cognitive limitations, we must ask whether employees really understand the rules. Stress can also cause people to make errors because it reduces their attention span and the capacity of their working memory.[6]

Key Dismukes and his colleagues argued that you need to understand these interactions so that you can address the real reasons for errors.[5] Charles Perrow maintained that the human actor isn't the sole source of the problem; you must also consider the system.[7] A system comprises employees, policies, processes, technology, and myriad other parts, which interact with and impact each other in multiple ways. When the system doesn't function optimally, untoward events (such as information breaches) occur. You must study the entire system to uncover the real antecedents, not focus on one specific part (that is, the person) where the abnormality manifests itself.

For further reading on noncompliance, visit http://doi.ieeecomputersociety.org/10.1109/MSP.2011.157.

References

1. E.M. Madigan, C. Petrulich, and K. Motuk, "The Cost of Noncompliance: When Policies Fail," *Proc. 32nd Ann. ACM SIGUCCS Fall Conf.* (SIGUCCS 04), ACM, 2004, pp. 47–51.
2. M.E. Thomson and R. von Solms, "Information Security Awareness: Educating Your Users Effectively," *Information Management & Computer Security*, vol. 6, no. 4, 1998, pp. 167–173.
3. G.A. Cohen, *Rescuing Justice and Equality*, Harvard Univ. Press, 2008.
4. P. Mascini, "The Blameworthiness of Health and Safety Rule Violations," *Law & Policy*, vol. 27, no. 3, 2005, pp. 472–490.
5. K. Dismukes, B.A. Berman, and D. Loukopoulos, *The Limits of Expertise: Rethinking Pilot Error and the Causes of Airline Accidents*, Ashgate, 2007.
6. J.E. Driskell and E. Salas, *Stress and Human Performance*, Lawrence Erlbaum, 1996.
7. C. Perrow, *Normal Accidents*, Princeton Univ. Press, 1999.

The board appointed information governance officers to visit the various sites to speak to employees, ensure that directives are applied, identify difficulties, and monitor the state of information governance.

Strong Management Support

Mark Thomson and Rossouw von Solms posited that senior management are crucial in cultivating a culture of information security.[4] The NHS managers appear to be fully committed to information security, being well aware of the NHS's past failings. (For more information, see the "National Health Service Security" sidebar.)

Survey Background

To capture the employees' perspective of the health board's information security policies and practices, I conducted an online survey. I chose an online survey because it would ensure respondents' anonymity, which I hoped would lead to honest, open responses. I created the survey with SurveyMonkey (www.surveymonkey.com) and tailored it to prevent duplicate submissions from the same IP address. The survey ran from June to August 2010. Each week until the survey closed, all board staff received a link to the survey, together with an explanation of the survey's purpose, as part of a staff-briefing email.

The Respondents

Of the estimated 5,000 employees on the mailing list, 328 responded to the survey. This relatively low response rate is to be expected in an organization in which most staff members use their computers only sporadically during their workday. Of the 328 respondents, 19 percent were male and 81 percent were female, which is representative of the gender balance in Scotland's NHS. Regarding the respondents' ages, 5.18 percent were in their 20s, 17.38 percent were in their 30s, 36.59 percent were in their 40s, 36.59 percent were in their 50s, and 4.27 percent were 60 or older.

Regarding the respondents' experience, 77 percent of them had been working for the board for more than six years, 4 percent between four and six years, 7 percent between two and four years, and 12 percent for two years. No respondents had worked for the board for less than two years. These numbers aren't particularly significant but do indicate an established staff that would have knowledge of the policies and system.

Limitations

One limitation of this study could be that someone who shared a machine with another person couldn't participate if that person had already used that computer for the survey. Also, online surveys are imperfect. Respondents could lie or respond in what they felt was a socially acceptable fashion, and a survey might attract only the most discontented staff members.

However, for this study, anonymity's benefits far outweighed these limitations. The study aimed to identify trends, gather anecdotes, and detect problems. For these purposes, an online survey was the best tool.

Noncompliance Risk Factors

Part of the survey attempted to find evidence of noncompliance risk factors, which might involve rules that are a nuisance, pose an ethical dilemma, or are impossible to follow.[5] Measuring overall policy compliance is difficult, but by examining password use, we can obtain some sense of whether employees adhere to policies. The health board's password policy included these rules:

- passwords must not normally be written down;
- passwords must not relate to the system being accessed;
- passwords must not relate to the user;
- employees can't use the same password on multiple systems; and
- employees must not tell anyone else their passwords.

These rules (except the last one) prohibit well-known coping skills people employ when confronted with too many passwords.[6] This suggests that they fall into the "impossible to follow" rules.

Following Password Rules

The survey listed five coping techniques and asked whether the respondent employed any of them.

National Health Service Security

The UK National Health Service (NHS) puts much effort into ensuring information security by following the recommendations of organizations such as the Computer Security Institute. Despite this, a response to a freedom of information request in 2008 reported that the NHS had potentially exposed more than 10,000 patient records since 2006.[1] In April 2010, *NHS Online* reported that since the end of 2007, the NHS had experienced 287 breaches.[2] Other reports claim that the NHS is the UK's worst offender in terms of information losses.[3]

References

1. L. King, "NHS' Grim Catalogue of Data Breaches," *ComputerWorld*, 26 Nov. 2008; www.computerworlduk.com/news/it-business/12126/nhs-grim-catalogue-of-data-breaches.
2. "NHS Guilty of More Data Breaches Than Any Other UK Organisation," *NHS Online*, 29 Apr. 2010.
3. I. Grant, "NHS Is Worst Offender as Reported Data Breaches Hit 1,000, Says ICO," *ComputerWeekly*, 28 May 2010; www.computerweekly.com/Articles/2010/05/28/241396/NHS-is-worst-offender-as-reported-data-breaches\-hit-1000-says.htm.

Table 1. The popularity of different password coping techniques.

Coping technique	Users (%)
Write passwords down	33
Reuse passwords	63
Use the system name	10
Use own username	19
Use month and year	7

Results. As Table 1 shows, some percentage of the respondents used at least one of the coping techniques.

Discussion. Research shows that people can't adhere to stringent password policies in the face of multiple passwords, especially when passwords change frequently.[6] Moreover, Dinei Florêncio and Cormac Herley found that users have an average of six and a half passwords, often shared across sites.[7] Employees aren't being perverse by reusing passwords; they're simply being human.

Mandating the impossible can frustrate employees, to say the least. It can negatively affect their attitudes to other policy directives, thus increasing noncompliance.

Despite stringent rules such as the health board requires, people still seem to use the same coping mechanisms they always have for unrealistic demands on their cognitive and memorial abilities. This noncompliance isn't due to the rules' nuisance value; the rules are clearly impossible. Users abandon the rules because they're futile.

There's an unfortunate impasse between the widely accepted demands of "good security," as encoded in the policies, and the equally widely accepted limitations of human users. It would be helpful if the board stopped forbidding and started assisting. The reality is that people will write down their passwords and use passwords they can easily remember, even though other people can probably easily guess them. It would be better if the board provided a sanctioned coping mechanism. A password-storing application would be a good start: it would remove the memorial load from the users and perhaps encourage them to use stronger passwords.

Password Sharing

The survey asked, "What kind of emergency would make you consider sharing your password with a trusted colleague?" The question included examples of possible scenarios, such as a medical emergency, an appointment needing to be arranged, or the responsible person being away. (The nature of these isn't important; the list's purpose was to give respondents ideas of scenarios in which they might consider sharing passwords.)

Results. Of the respondents, 63 percent indicated that they would be willing to share if the justification was sufficiently compelling.

Respondents also volunteered possible justifications. Some responses were related to the employee being away; here are some examples:

- The employee is on vacation, and a client needs access to a report.
- The employee suddenly becomes ill, and another employee needs a file that hasn't been uploaded to a shared drive.
- Information is suddenly needed for a meeting, and that information's unavailability would cause the meeting to be delayed or canceled.
- The employee is on long-term sick leave.

Some responses were related to deference to managers, such as if a senior manager requires information that's not on a shared workspace. One respondent said, "I never give my passwords away to colleagues, but would let my supervisor know if it was needed in an emergency."

Some responses were related to operational difficulties or realities; here are some examples:

- When the company takes too long to incorporate new hires into the IT system, colleagues sometimes share passwords with them so that they can start their work.
- Employees can experience technical difficulties that must be resolved by support staff, who are sometimes engaged elsewhere; they often give their passwords to facilitate this.
- Sometimes, a system that the respondent had originally logged on to was also used by others and needed to be restarted. So, the respondent talks a colleague through entering the respondent's password (but isn't overly concerned that the colleague will later remember the entire password).
- A secretary needs access to correspondence (which he or she would have already had access to in a paper system).

Some respondents said they'd share passwords only in real emergencies. Others said they would be willing to share passwords only if there was a provision that ensured them no guilt, such as a senior manager authorizing it in writing.

On the other hand, 15 percent of the respondents stated that they wouldn't share passwords, with some of them using stark wording (for example, "none" or "never share").

Four respondents who said they would share also suggested sanctioning a sharing mechanism. For example, people should be allowed to share when they feel the justification is compelling enough but must change the password immediately afterward.

A significant number (22 percent) of respondents didn't answer this question, perhaps because they didn't trust the survey's anonymity.

Discussion. The board is unequivocal about password sharing: it's not permitted. Yet this edict conflicts with what's known about human nature and the realities of group working. Information sharing is vital in group work settings.

Furthermore, cohesive groups deliver superior performance. As a group's cohesion develops, its members start to empathize, self-disclose, and accept and trust each other. People who work together thus become accustomed to working collaboratively and trusting each other and sharing information. Asking them not to share passwords creates an ethical dilemma between a desire for the group's common good and compliance with the security policy. Joan Finegan said,[8]

> When an individual is faced with an ethical dilemma, his or her value system will colour the perception of

> the ethical ramifications of the situation. For some individuals, the behaviour in question might be in clear violation of their organization's code of ethics; for others faced with the same situation, the behavior might be seen as quite acceptable.

The nonsharing policy is one that employees won't comply with; wise administrators will abandon it or soften the requirements.

The four respondents' proposed compromise might not sit well with current security policies. However, it would let people help trusted colleagues and build a working environment more conducive to cooperation and collaboration. It's also more realistic. The reality is that people share passwords. It would be better to offer a sanctioned way of sharing, thereby offering control of this inevitable behavior.

Mistake Risk Factors

The rest of the survey dealt with mistake risk factors, which involve the following questions. How stressed do employees feel, and how does this stress make them react to policy changes? Do they understand the policies, and how do they feel about them? What task demands seem at odds with the policy requirements? Finally, what environmental factors play a role?

Stress Levels and Policy Formation

One question gauged the extent to which employees felt they were overextended.

Results. Figure 1 shows the responses. Most employees seemed to be coping with their jobs, although more employees indicated high stress levels than low.

The survey also asked how respondents would react to a policy requiring them to change how they did something. The response options included *no problem* (22.4 percent), *despair* (4.8 percent), *feeling resigned* (18.4 percent), *not another change!* (44.2 percent), and *how am I going to keep up with these changes?* (36.4 percent).

Policy formation. One part of the survey was only for managers and dealt with policy formulation. (The health board currently doesn't involve nonmanagers in this process.) The survey asked, "Would you like to be able to engage in, and input into, the contents of the policies?" The options ranged from *strongly disagree* (1) to *strongly agree* (5). The mean response was 4.06; the median and mode were both 4 (*agree*), indicating a generally strong agreement with the statement. Of these respondents, 86 percent either agreed or strongly agreed—so the majority did indeed want to be involved in the process.

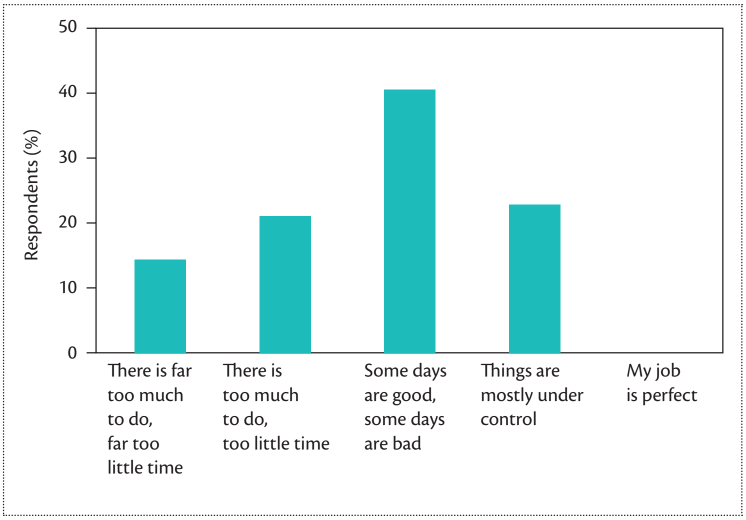

Figure 1. Results for the survey question, "When you think about your job, you think that …." The skew is 0.342, which gives cause for some concern because stressed employees will more likely make mistakes.

The next question asked how the respondents would like to be involved. The responses were *email* (68.1 percent), *via a webpage* (38.5 percent), *meetings* (16.5 percent), or *visits from officers* (17.6 percent).

Discussion. The skew (asymmetry) in Figure 1 gives cause for some concern because stressed employees will more likely make mistakes.[9]

As I mentioned, most respondents responded negatively to the idea of additional policy edicts changing their current behavior. You might be tempted to dismiss this as mere resistance to change. Matters aren't that simple, however. Eric Dent and Susan Galloway Goldberg argued that people don't resist change as a matter of course; they resist things such as loss of status, loss of pay, or loss of comfort.[10] Perhaps, in the survey's context, the respondents were resisting more curtailment of their activities and more restrictions, all of which make their workday more difficult ("nuisance" rules). Certainly some of the responses suggest this. Respondents used "restrictive," "encumbrance," "frustrating," and "unworkable" to describe the policies. If employees already feel overly restricted, it's not surprising that they might react negatively to yet another edict.

There's no simple solution to this: those higher up in the hierarchy are pressured to prevent information breaches, and they use the tools at their disposal. In many cases, policies are their best, if not only, tool. However, many of the respondents' comments suggest that staff feel the people who compose the policies don't understand the jobs' realities, suggesting that the policies might fall into the "impossible to follow" category. As I mentioned, most managers expressed willingness to be involved in policy formulation. In expressing a preference for email, they're perhaps indicating that this involvement should be as convenient as possible.

Karin Höne and Jan Eloff argued that employees will gain a broader understanding of security issues, and thereby improve secure behavior, if security policies are developed in conjunction with stakeholder representatives.[11] J. Kenneth White and Robert Ruh demonstrated a significant positive correlation between increased participation in decision-making and job attitudes.[12] Perhaps this is the best way of closing the gap between the policy writers and the employees that these policies impact.

Relating to the Policies

Of the respondents, 49 percent found the policies ambiguous, and only 12 percent thought they were clear. The rest chose the middle option, choosing not to commit themselves in either direction.

The survey also asked respondents to give "one word or phrase to describe the information governance policies." Of the 222 descriptions gathered, 133 (60 percent) were positive and 89 (40 percent) were negative. The most common positive responses were "necessary," "beneficial," "essential," "OK," and "good." The most common negative responses were "obstructive," "nuisance," "no trust," "unrealistic," "out of touch," "irrelevant," "restrictive," and "complex." Because the survey framed the question in terms of the policies' clarity, I classified the one-word responses in terms of how each word related to the document's clarity.

Two respondents questioned the motivation for the policies. One said the policies were "generally useful, although often … they're used as 'back-covering' to place the blame on clinicians when things go wrong." Another said they were "a huge bureaucracy to solve a problem that is of more concern to politicians and the media than it would otherwise be to the public."

Other respondents mentioned concerns such as staff being absent when new policy changes are introduced, experiencing confusion on protocol for breaches, and having limited understanding of the actual policies owing to their complexity.

Regarding the negative responses, a number of respondents complained about the policies being complex, difficult to interpret, ambiguous, complicated, or vague. We must consider that any large organization will have employees of widely varying literacy. Policy writers should make their policies as accessible as possible to all employees. One widely accepted tool is the Fog index, which can give some indication of a document's readability. Adrian Bauman and his colleagues showed that health-related education materials were far more complex than the typical newspaper (which is written for the general public).[13] Organizations should aim to disseminate policy documents that are at least as readable and understandable as a newspaper article.

Although this addresses understandability, it doesn't address the complaints that the policies are too restrictive, out of touch, obstructive, and so on. Some of these criticisms are related to the core rationale for policies—they must restrict and constrain by nature. Paul Slovic and Amos Tversky argued that if people understand a principle better, they're more likely to behave in accordance with it.[14] Perhaps the dissemination of policies could more effectively explain the rationale behind some of the rules.

Finally, a number of people used "nuisance" to describe the policies. We can't expect them to state that they deliberately ignore "nuisance" rules, but this kind of response should raise concerns.

Unrealistic Task Demands

Many respondents said that although the policies were good in theory, it wasn't always so black and white for various circumstances. One respondent said, "The policies are great in principle but a different matter when you are working in a busy environment where you are working to deadlines and under pressure." Respondents said some policies don't recognize demands, some are unrealistic without sanctioned workarounds available, and some simply must be ignored to get work done. One respondent thought that no clinicians had been involved in the policymaking; if they had been, they would have made life easier.

Policies must accommodate the needs of all staff. The solution might well be, as I suggested earlier, to involve stakeholders from all different roles across the health board in formulating the policies. These comments suggest a measure of alienation, which I'm sure the health board doesn't intend and which they would do well to address.

Environmental Factors

The survey asked how adequate the support was for policy implementation. The options ranged from *processes always work* (1) to *significant problems* (4).

Results. The mean response was 2.25, with a mode and median of 2. Of the respondents, 13 percent indicated that there were significant problems and 85.9 percent felt the process worked most of the time.

Additional comments from this section indicate that there were indeed problems with operational support, ranging from inadequate telephone call data to malfunctioning hardware. One respondent mentioned a request for a USB stick over a year earlier that the organization still hadn't fulfilled.

Discussion. It might seem obvious, but it's worth emphasizing: Organizations can't impose processes and procedures without providing the resources to support them.

This health board could be atypical, but most likely it isn't. Reports of information breaches proliferate across health boards, so the experiences and emotions reported here are likely duplicated in health boards.

Given the anecdotal evidence, it's no surprise that information breaches still occur. To address these, organizations must consider the whole system. Firing the single employee who falls foul of circumstances and causes a breach often contributes little to resolving the situation.

Asaf Degani wrote about the tendency to blame pilots for airline crashes. He argued for "a more scrupulous perspective to pilot error" that duly considers human and technological factors.[15] Surely it's time for security professionals to embrace this approach, too. The time for blaming and shaming has passed. Organizations must meet nonsecurity employees' needs while still meeting information governance requirements. The current situation is clearly undesirable, with many employees exhibiting emotions akin to resentment and discontent. It's time for a new era in information security management, in which human needs are understood and accommodated rather than scorned and dismissed. ■

Acknowledgments

I thank the health board's information governance staff for their support and Wendy Goucher for her contributions in formulating the questionnaire. My thanks to Heather Crawford and Tim Storer for their comments on an earlier draft of this article. Finally, I thank the anonymous reviewers for their helpful comments.

References

1. *CSI Computer Crime and Security Survey*, Computer Security Inst., 2009.
2. P.F. Drucker, "Management and the World's Work," *Harvard Business Rev.*, Sept. 1988, pp. 65–76.
3. C. Vermeulen and R. von Solms, "The Information Security Management Toolbox—Taking the Pain out of Security Management," *Information Management & Computer Security*, vol. 10, no. 3, 2002, pp. 119–125.
4. M.E. Thomson and R. von Solms, "Information Security Awareness: Educating Your Users Effectively," *Information Management & Computer Security*, vol. 6, no. 4, 1998, pp. 167–173.
5. P. Mascini, "The Blameworthiness of Health and Safety Rule Violations," *Law & Policy*, vol. 27, no. 3, 2005, pp. 472–490.
6. A. Adams and M.A. Sasse, "Users Are Not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures," *Comm. ACM*, vol. 42, no. 12, 1999, pp. 40–46.
7. D. Florêncio and C. Herley, "A Large-Scale Study of Web Password Habits," *Proc. 16th Ann. Conf. World Wide Web* (WWW 07), ACM, 2007, pp. 657–666.
8. J. Finegan, "The Impact of Personal Values on Judgments of Ethical Behaviour in the Workplace," *J. Business Ethics*, vol. 13, no. 9, 1994, pp. 747–755.
9. J.E. Driskell and E. Salas, *Stress and Human Performance*, Lawrence Erlbaum, 1996.
10. E.B. Dent and S. Galloway Goldberg, "Challenging 'Resistance to Change,'" *J. Applied Behavioral Science*, vol. 35, no. 1, 1999, pp. 25–41.
11. K. Höne and J.H.P. Eloff, "What Makes an Effective Information Security Policy?," *Network Security*, June 2002, pp. 14–16.
12. J.K. White and R.A. Ruh, "Effects of Personal Values on the Relationship between Participation and Job Attitudes," *Administrative Science Q.*, vol. 18, no. 4, 1973, pp. 506–514.
13. A.E. Bauman et al., "Asthma Information: Can It Be Understood?," *Health Education Research*, vol. 4, no. 3, 1989, pp. 377–382.
14. P. Slovic and A. Tversky, "Who Accepts Savage's Axiom?," *Behavioral Science*, vol. 19, no. 6, 1974, pp. 368–373.
15. A. Degani, "Pilot Error in the 90s: Still Alive and Kicking," keynote address at 44th Ann. Meeting Flight Safety Foundation/Nat'l Business Aviation Assoc. (FSF/NBAA 99), 1999; http://ti.arc.nasa.gov/m/profile/adegani/Pilot%20Error%20in%20the%2090s.pdf.

Karen Renaud is a computing scientist at the University of Glasgow's School of Computing Science. Her research interests include the accessibility of security software improvement and the interplay between policies and employee behavior. Renaud received a PhD in computing science from the University of Glasgow. Contact her at karen.renaud@glasgow.ac.uk.