Business Horizons (2006) 49, 115—125

Available online at www.sciencedirect.com

SCIENCE DIRECT

INDIANA UNIVERSITY
KELLEY
School of Business

www.elsevier.com/locate/bushor

Y2K all over again: How groupthink permeates IS and compromises security

William Schiano *, **Joseph W. Weiss**

Bentley College, 175 Forest Street, Waltham, MA 02452, USA

KEYWORDS
Information systems;
Security;
Groupthink;
Software

Abstract Despite increased concerns about security, most government, private, and public information systems remain vulnerable to terrorist and hacker attacks. To examine this potentially catastrophic problem, we study another infamous, expensive failing in information systems: the year 2000 (Y2K) problem. We argue that many of the same drivers of the Y2K problem now impede the security of information systems, and identify *groupthink* as a root cause of the continuing inability of organizations and IS (information systems) teams to learn from past mistakes in managing information systems. We also identify measures to help organizational team leaders and members prevent future IS-related threats.

1. Overcoming groupthink

From client level viruses and spyware to large scale intrusions and denial of service attacks on servers and networks, security breaches in 2004 inconvenienced millions and cost billions of dollars. While security policy, strategy, and enterprise cultural responsibility reside with board members, CEOs, and CIOs, implementation relies on technology and cross-functional groups. Janis's well established and still popular concept of *groupthink* (the desire for affiliation and pressured consensus that impedes teams' critical evaluative capabilities) is most prevalent in teams and can facilitate serious electronic security lapses (Janis, 1983).

Many breaches are the result of users not following security policies, failing to secure passwords or inadvertently allowing access to unauthorized users. While hackers' and terrorists' attempts to disrupt systems present real threats, IS (information systems) professionals can also put entire organizations at risk by developing, marketing, implementing, and maintaining insufficiently secure software. Moreover, IS professionals are the gatekeepers who must detect, decipher, and act when electronic security is breached. We therefore address specific recommendations for overcoming groupthink at the technology leadership and group level. Nonetheless, without the active support of boards and officers, technology team leaders and members cannot be expected to care about or protect the organization.

* Corresponding author.
E-mail addresses: wschiano@bentley.edu (W. Schiano), jweiss@bentley.edu (J.W. Weiss).

0007-6813/$ - see front matter © 2005 Kelley School of Business, Indiana University. All rights reserved.
doi:10.1016/j.bushor.2005.07.002

Recent security breaches are not the first time information systems have been seen as a threat. The Y2K problem was estimated to cost over $400 billion to remediate, and many fear if the problem had not been addressed, it could have crippled the world economy. We explore how the Y2K problem arose and argue that, due to groupthink, many of the same mistakes that led to the Y2K crisis are causing gaps in computer security today.

2. Groupthink and electronic security

Because of groupthink, many of the causes of Y2K persist and compromise electronic security. IS officers publicly recognize the technical failings of the Y2K debacle while admitting the current non-secure status of electronic systems in general. Our work with IS teams, in particular, shows that most have strong feelings of loyalty to their work-groups and only privately question the validity of any member's disgruntled claims about security. Critical thinking is obviated when groupthink is reinforced by team leaders and members. The desire to keep the group intact and remain a member can result in poor and even dangerous group decisions.

Surprisingly, IS researchers have not linked groupthink to Y2K or electronic security issues. We surmise this omission relates to researchers' focus on improving "IS and business alignment"; i.e., the need to get organizational professionals thinking and acting more alike. By acknowledging and addressing groupthink as a root cause, IS departments can break the cycle of crisis and address business needs effectively.

2.1. Antecedent conditions of groupthink: The IS context

In addition to the existence of a cohesive group, Janis cites two categories of groupthink-facilitating antecedent conditions that are also relevant to IS teams. The first category, *structural faults of the organization*, is indicated by such factors as:

(1) Insulation of the group;
(2) Lack of tradition of impartial leadership;
(3) Lack of norms requiring methodical procedures; and
(4) Homogeneity of members' social background and ideology.

IS organizations are susceptible along this dimension; they are often isolated geographically due to outsourcing, or in order to save on real estate or be located closer to the hardware. They are apt to develop a culture different from the rest of the business (Capretz, 2003), and often struggle with poor management (Glaser, 2005) in a profession that is more than three-quarters male (Information Technology Association of America, 2003).

The second category of antecedent conditions, *provocative situational context*, is indicated by factors such as:

(1) High stress from external threats;
(2) Low self esteem induced by factors such as recent failures and excessive difficulty in making decisions, lowering each member's sense of self-efficacy; and
(3) Moral dilemmas reflected in an apparent lack of feasible alternatives except ones that violate ethical standards.

Again, IS organizations are susceptible: pressure from the business is continuous, the perceived failure rate of IS projects has been estimated as high as 75%, and there is a standing belief in many companies that IS projects are routinely buggy, late, and over budget.

3. Y2K all over again

Y2K may be over, but underlying groupthink symptoms remain, making teams and organizations vulnerable to electronic security threats. While enterprise boards, leaders, policies, and strategies are needed to support security prevention efforts at divisional and lower levels (Dutta & McCrohan, 2002; McAdams, 2004), groupthink occurs and must be addressed within technical and cross-functional teams. This was the case with the Y2K crisis, and now applies to electronic security threats. Supported by practitioner and academic studies, our consulting experience points beyond technical and accidental factors as major and single causes of the Y2K crisis and electronic security glitches. For example, CSC Research (1997) listed five causes of the Y2K problem:

(1) Designing systems on the assumption that resources are scarce;
(2) Doing just what the business asked for;
(3) Not following architectural standards;
(4) Putting off the problem; and
(5) Hardcoding; i.e., writing software with immutable behavior that can be changed only by replacing lines of code.

Table 1 Mapping IS and groupthink symptoms

Groupthink symptoms (Janis, 1983)	Type I overestimation of the group		Type II closed-mindedness		Type III pressures toward uniformity			
IS symptoms (various)	Illusion of invulnerability	Belief in group morality	Rationalization	Stereotyping	Self-censorship	Illusions of unanimity	Pressure on dissenters	Mind-guarding
Assuming resources are scarce			✓		✓	✓	✓	✓
Just doing what the business asked for			✓		✓	✓	✓	✓
Not following standards	✓		✓	✓				
Putting off the problem	✓		✓				✓	
Hardcoding	✓		✓				✓	
Culture	✓	✓	✓	✓	✓	✓	✓	✓
Applications as temp.	✓		✓					✓

Thomsett (1998, p. 91) added two additional causes: "a well established culture that viewed programming as a private, creative art form", and "a then-reasonable and widely held belief that the systems and code being written would be replaced within ten years". We show how these problems routinely result in security shortfalls.

Table 1 illustrates how Janis's eight symptoms of groupthink correspond to the seven enduring problems mentioned above. The following sections outline how each of these seven factors contributed to the Y2K problem, and how security development and implementation are repeating these mistakes as a result of groupthink.

3.1. Designing systems on the assumption that resources are scarce

The most obvious perceived resource constraint for Y2K systems was storage space. From the days of eighty column cards, developers of non-Y2K compliant systems used only two digits for the year to conserve space. The resulting problems are well known. Hardware and software budgets, staffing limits, and support for maintenance were also perceived as constraints.

The assumption that resources are scarce did not vanish in 2000. The dot-com crash increased focus on profitability and IS budgets have failed to keep up with inflation (Bartels, 2004), causing hesitation to spend on non revenue-generating projects. While security spending has risen, it is still only in the single digits as a percentage of IS budgets (Penn, 2004). Further, spending per employee varies widely by industry, from $106 in metals/natural resources to $7,022 in energy/utilities (Berinato & Ware, 2004).

Success of security efforts is difficult to measure (Power, 2003), and many organizations are using financial models to compensate. Gordon, Loeb, Lucyshyn, and Richardson (2004) found that 55% of companies used ROI to evaluate security spending. Avoided costs are used in lieu of revenue; however, a study by Koetzle (2003) found that 60% of firms did not know what security breaches had cost the company in the previous year, making it unlikely that firms can accurately calculate avoided costs. The use of formal models provides false precision and, in some organizations, impedes a more careful security analysis. Relying only on technical and financial models to explain broader issues in group decision-making processes does not address the underlying causes of past Y2K problems or current security threats.

Groupthink symptoms related to assumed resource scarcity include rationalization, self-censor-

ing, and lack of critical thinking. For example, one underlying rationalization is that resources have always been scarce and will continue to be so; therefore, it is easier to assume the scarcity. Another rationalization is that by operating frugally and not seeking additional resources, the IS group is serving business interests. In most organizations, IS is a cost center, so minimizing costs is a major driver.

Given the widely held assumptions regarding scarcity of resources and the accompanying level of frustration with constraints, IS professionals often self-censor to avoid being seen as complainers. Fear of being blamed for other unexplained past problems could lead team members to self-censor on current issues. Scarcity of resources is a recurring problem that can (and does) disguise other, more serious problems like security lapses from surfacing in meetings.

Along with an assumption of scarce resources, the lack of business understanding and savvy on the part of many IS professionals contributes to a willingness to accept constraints quickly, without challenging them appropriately. This lack of critical thinking is another precondition of crisis mode activity (or inactivity) surrounding security threats.

The assumption of resource scarcity also promotes a culture where proposals beyond perceived resources are discouraged. In addition, resource allocation discussions are generally limited to management; consequently, restrictions are often simply assumed.

3.2. Just doing what the business asked for

Until the 1990s, few, if any, business units requested systems that were Y2K compliant. Rather than looking beyond the immediate demands of the business, IS departments simply did their best to meet requests, many of which often exceeded the resources and abilities of the group. Even when IS knew of problems and felt strongly that they needed to be addressed, IS lacked the authority to implement changes the business found too costly.

Business units in most organizations are not interested in the inner workings of information systems. As systems grow to be more complex, it becomes increasingly difficult for those outside IS to understand the implications of their requests. A *CIO* magazine poll found that over 80% of organizations have a backlog of applications to develop (Yardeni, 2005). Exceeding business requests would only add to this surfeit. With the advent of electronic commerce, technological risks have increased. Systems must now be accessible to users outside the organization, including suppliers and customers. And while external visibility has created some pressure to improve the quality of systems, this is often outstripped in many organizations by pressure for fast changes and quick fixes.

For security precautions to succeed, users are (and must be seen as) a crucial component. Without company support, IS stands little chance of enforcing meaningful security policies. Developers and project managers see little incentive in expending the time and resources necessary to insure against future problems, even if these problems can be identified. The primary mandate in many organizations is, "just launch". A Cutter Consortium (2001) study of e-projects found 43% of respondents cited "high functionality" as the primary goal, while only 34% said "high quality". Such short-term focus makes finding support for investments in scalability and security difficult.

Even when business is not short-sighted regarding security, there are inevitable tradeoffs in terms of accessibility and responsiveness. For their part, responsible managers must make such compromises. Unfortunately, large numbers of those involved in IS lack formal training in security matters (Peck, 2003), making identifying and analyzing these tradeoffs even more difficult.

Related groupthink symptoms of "just doing what the business asked for" include all of Janis's pressures toward unanimity about project scope, avoiding protracted, uncomfortable battles that can uncover disturbing information (e.g., about lack of security precautions). This is rationalized as being responsive to the business. Doing only "what the business asked for" reflects pressure to not expand the scope of work and stems in part from an effort to prevent hearing other ideas.

3.3. Not following architectural standards

In a history of the Y2K problem, Williams and Smyth (1999) documented that standards for four digit dates were well established in the early 1970s, and that there were many warnings about the Y2K problem within the IS community throughout the 1980s and early 1990s. Facing tremendous pressure from businesses for new applications, system developers often saw standards and methodologies as a hindrance, and continued to use two digit dates. Even when methodologies were used and standards were adhered to, there was substantial variance in the construction and documentation of systems.

Similarly, standards for security have existed for decades (Baskerville, 1993), and are not a panacea. The compromises and complexity necessary for the

creation and adoption of security standards may lead to security shortcomings (Mercuri, 2003). This requires greater judgment from those applying the standards; however, security is often not a required topic in professional training programs (Anderson & Schwager, 2002), leaving even those with IS degrees lacking in crucial knowledge. Increasing compliance with security standards could limit functionality and would certainly increase costs.

Security is the domain of more than any one system. As the need for systems integration continues to increase within the organization and beyond its boundary to suppliers and customers, this problem is amplified. Even if standards are followed in some areas, if they are not enforced in all, breaches are likely. This increases the necessity of preventing security lapses in any and all systems, now.

While the dot-com collapse depressed the volume of IS staff departures, most organizations expect the high turnover rates of the last decade to return (Surmacz, 2004). Unfortunately, employee turnover exacerbates the problems of enforcing standards.

In many professions, not following standards would likely lead to catastrophic career consequences. Many IS professionals, however, believe they are beyond attack, both because of the isolation of their work and the fact that they will often be gone before any shortcomings are discovered. It is common to hear tales of superstar developers who are permitted to work outside the rules because they are more productive than average team members. Our observations of cross-functional IS teams (including programmers) confirm that creative, productive "stars" generally view themselves as artistic and technical experts, whose judgment and experience are beyond common criticism. While most groups did not share the same illusion of invulnerability, we did notice that several stars were able to, and did, exert influence over key decisions.

The ignorance of standards is rationalized as expedient, therefore serving the needs of the business. It also shows a level of disregard and, in some cases, contempt for the clients, who are often stereotyped as ignorant of technology issues.

3.4. Putting off the problem

Many organizations postponed Y2K work until the late 1990s, generating a crisis. Few within IS departments saw benefit in leading Y2K initiatives until things reached crisis proportions; after all, such initiatives would have been seen as costs rather than contributions. No one outside IS was asking for them and they would not generate revenue; thus, team leadership was hardly seen as a career advancing move.

Though Y2K has come and gone, the backlog of work in most IS departments remains, and client disinterest in long-term and internal issues has changed little. Components and agile development methodologies have only further whet the dangerous appetite for systems to be developed and launched more quickly. Like Y2K projects, security also suffers from the same lack of revenue generation and correlated neglect. Except for those specifically employed in positions devoted to the concern, few see incentive in taking responsibility for security.

Of course, the focus on security naturally increases after breaches or other crises. Given various organizational pressures, however, maintaining vigilance is difficult, particularly since increasing security often means delays, increased expense, reduced accessibility, and poorer usability.

"Putting off the problem" often includes several groupthink symptoms: sense of invulnerability, rationalizations, and pressure on dissenters. A company's lack of understanding of what IS does and high staff turnover foster a sense of invulnerability. IS departments rationalize procrastination by emphasizing the importance of the work at hand. Any team member who advocates delaying immediate technical issues to solve a complex, long-term, and potentially more serious security issue without the leader's support risks becoming a dissenter.

3.5. Hardcoding

The difficulty of locating and fixing date problems in Y2K code is well known. Long regarded as a poor programming practice, hardcoding (making changes to programs that can only be undone by editing the code itself) was frequently done because it is expeditious. Sanders (1998) notes that many non-Y2K compliant systems were written from scratch. While far fewer systems are written from scratch today, many Web systems were and still are. Even companies using ERP software still customize much of the code, and have difficulty enforcing policies against hardcoding.

Hofmeyr (2003) notes that security hardcoding is common. Because of the pressures already described, many IS organizations spend a great deal of time putting out fires. A quick, hardcoded patch can relieve a pressing problem, but such quick fixes may not work when software is upgraded or systems are migrated. The lack of documentation among many systems also compounds the difficulty.

Most organizations recognize the importance of keeping up with immediate pressures but do not look to the future, reflecting a conscious and sometimes nonchalant sense of invulnerability on the part of IS executives and professionals. In addition, hardcoding is rationalized as expedient. While the pressure to conform may not be explicitly to hardcode per se, there is tremendous pressure to do what is necessary to meet deadlines.

3.6. Culture

Many of the non-Y2K compliant systems were written at a time when development was dominated by a maverick mentality. Limited mainframe access created a power dynamic that led to feelings of invulnerability on the part of IS professionals. Business units were mystified by how the technology worked, and had to ask for reports from routinely separated IS departments. Programmers viewed themselves as different from the rest of the business, a view the business shared. Computer professionals also hold a utopist vision of technology; therefore, many were less fearful about the Y2K problem than overreacting, non-technical people (Tapia, 2003). This is consistent with Schein's (1996) finding that technologists assume they can master nature and prefer "people free" solutions.

This unique IS culture remains. But, like the Y2K problem, security is largely a management, not a technical, issue (Dutta & McCrohan, 2002) and requires the development of a culture of security (OECD, 2002). Reflecting the gap in the culture of security, one *CIO* magazine survey established that only 28% of security professionals found security considerations a routine part of the business processes of their companies (Yardeni, 2005). Complicating the development of such a culture is the fact that no usable system can be completely secure; the enduring myth of secure computing must be combated (Austin & Darby, 2003). The belief that users of Web systems are more tolerant of errors has also contributed to the lax attitude toward testing and security (Pressman, 2000). As well, many IS departments resist introspection and avoid opportunities (e.g., post-project reviews) to evaluate weaknesses.

Much of the discussion of security is framed around fear. A 2003 survey found that 69% of respondents justified their investments in security by liability, while only 36% cited contribution to business objectives (Berinato & Ware, 2003). This finding emphasizes the need for more openness in technology teams, which would better enable programmers to share their knowledge, ideas, and expertise in attempt to uncover and solve glitches and preventative solutions. We have been repeatedly told by programmers and technology team members that they do, in fact, identify questionable security symptoms and take corrective action. Others, however, do not act to prevent or solve security-related glitches if they are under time constraints or are unsure of a solution.

The historic physical, educational, and cultural separation of IS from the rest of business fosters the groupthink symptom of members' sense of invulnerability. The rise of outsourcing, particularly offshore, has demonstrated vulnerability, and many professionals feel threatened. Nonetheless, pride and arrogance in ability remain strong in many organizations.

Also, the widely held view of IS as arrogant and dismissive reflects the groupthink belief in the group's morality. Many IS professionals feel more pressured to believe in the goals, plans, and deadlines of their bosses and executives than those of their own workgroups. The group morality derives more from the top than the bottom of the IS organization, especially when IS projects and initiatives are viewed as a competitive advantage or cost containment necessity.

In addition, IS cultures reinforce rationalization by discouraging analysis, especially after projects have been completed. The general culture of IS routinely portrays the business side as inept luddites. In many organizations, IS and business professionals exhibit reciprocal negative labeling, especially during periods of high stress when deadlines loom. The continuing problem of internal organizational IT and business alignment may be partially explained by stereotyping among groups. Moreover, many managers drive the organization's and their own career agendas while closing off open communication. A resultant top-down closed culture reinforces the suppression of information and two-way communication, another precondition in this context for groupthink.

Finally, a closed culture encourages an "us-versus-them" mentality that leads to quick unanimity, and to in-group versus out-group formation. The culture also creates pressure to conform, in part by emphasizing the need to be seen as a united group.

3.7. Applications as temporary

From the 1960s through the 1990s, developers believed the systems they were building would not still be in service in 2000, thinking business needs and technological advances would, by then, have rendered them obsolete. In many cases,

businesses explicitly claimed systems would be replaced by the year 2000. This made Y2K compliance a minor issue, if not entirely irrelevant, at the time of system construction.

Web-based systems are often constructed as if they are prototypes. The combination of ease of rapid development, heavy client involvement in specifications, high perceived tolerance for errors in Web systems, regular updates, and pressure to launch quickly lead to hasty construction. Once an organization, its customers, or suppliers become reliant on a system, it becomes difficult to replace and incremental change becomes the norm. The evolution of agile development methodologies exacerbates this trend, and makes building in security less attractive.

The view of applications as temporary has increased the groupthink symptom of invulnerability, since users have become more tolerant of shortcomings. Some IS organizations, where quality assurance has often played a limited role, even believe that errors are beyond their control. This view of applications as temporary is rationalized by accepting vague assurances that the system will be replaced and by the value of implementing the system quickly.

A view of applications as temporary also reflects team members' unwillingness to view the systems as long-term. This belief leads to IT workteams keeping at bay open discussions regarding wider concerns regarding security problems. False consensus (or an absence of any critical questions or discussion) about operating procedures and questionable programming practices are, again, susceptible to other groupthink symptoms that can lead to serious security oversights and breaches.

4. Overcoming groupthink

Just as they knew how to prevent and solve the Y2K problem decades before it became a crisis, IS executives and professionals know how to make systems secure. Publications addressing specific steps to secure systems and organizational and technical requirements are plentiful (for example, see http://csrc.nist.gov/). Recent trends to increase security within organizations are consistent with these recommendations; for example, many organizations are now creating or emphasizing internal audit groups, which can help provide external perspective. Larger IS organizations have policies and procedures for dealing with security lapses. An increasing number of these firms have also created chief security officers and separate security organizations reporting to senior executives (Berinato & Ware, 2004; Deloitte Global Financial Services Industry, 2004; Lohmeyer, McCrory, & Pogreb, 2002).

Nonetheless, the drivers that once caused Y2K problems and now compromise electronic security persist. The standard security enhancement recommendations in the academic and practitioner press must extend to all groups and levels of the organization, must be integrated into meetings, and must permeate the culture. Role and structure enhancements alone will prevent neither groupthink nor security crises.

As illustrated in Table 2, Janis offered nine recommendations for overcoming groupthink, all of which should be adopted by technical team leaders as part of their crisis prevention orientation and training. In our two decades of consulting and research, we have not seen this type or level of attention given to technical work teams with regard to crisis prevention of security threats.

As stated previously, several studies argue electronic security is an issue that should start at the board level and be driven by executive officers, in particular the CEO and CIO (Dutta & McCrohan, 2002; McAdams, 2004). We agree, but observed several large corporations that include security prevention in their governance policies and procedures without implementing specific prevention policies down to technical team operating procedures. Lessons inferred from groupthink show that unless technical team leaders are trained and rewarded for creating and sustaining critical think-

Table 2 Janis's recommendations for overcoming groupthink

1. Encourage the group to give high priority to airing objections and doubts.
2. As a leader, do not take a partial side to a point of view or course of action. Absent yourself from meetings to enable open discussion.
3. Set up separate groups to work on the same policy question.
4. Within groups, create subteams to work on the same problems; then, openly share proposed solutions.
5. Enable team members to discuss issues with outsiders and report their reactions back to the group.
6. Invite outside experts to observe and react to group processes and decisions.
7. Assign a member to play "devil's advocate" at each group meeting.
8. When the decision involves a rival organization, survey signals from rivals and construct alternate scenarios of their intentions.
9. Review decisions by holding "second-chance" meetings after consensus.

ing in a responsive organizational environment, boards and executive policies will not prevent serious electronic security threats.

Our post-9/11 discussions and informal interviews with technical team leaders and members suggest that potential crisis planning takes a back seat to daily pressures of "monetizing" work priorities and loads to meet profit and performance objectives. We also hear the recurring theme, "We really can't do a lot to prevent security attacks except keep anti-virus and spy software on high alert". There is a lack of concern for team process and awareness skills that encourage proactive prevention strategies and tactics.

5. Diagnosing groupthink security risks at the work team level

As illustrated in Table 3, we offer nine diagnostic questions technical team leaders and their supervisors can use to prevent groupthink and related security lapses and problems. These items can be applied to business, cross-functional, and technical teams. Explanations of each diagnostic question follow.

5.1. How high a priority is security for the leader and team?

Even the attacks of September 11 have done little to change computer security behavior. An Ernst and Young (2004, p. 7) survey found that only 20% of respondents strongly agreed their organizations "perceive information security as a CEO level priority". A CIO/PriceWaterhouseCoopers study found over 50% of organizations cited insufficient funding as a barrier (Berinato & Ware, 2004). A Deloitte Touche Tohmatsu study found that only 28% of organizations linked security to the performance evaluation of IT and security staff (Deloitte Global Financial Services Industry, 2004). As Harris Miller, president of the Information Technology Association of America notes:

"CEOs want their IT systems to be as fast as a Ferrari but as safe as an armored truck. Whenever tradeoffs arise, the bias is toward speed, not safety and security. . .(post September 11, 2001 security) is still not the priority we'd like to see. . .CEOs and CFOs are making a lot of tough choices of where and where not to spend money" (Paulson, 2002, pp. 10—11).

Miller's statement confirms our observations at the programming level, as well. Under the daily pressures of routine and special assignments, many technical team leaders and members react to rather than prevent or protect against programming and other computer-related security risks. These same leaders must be instructed and appraised to make security awareness and responsiveness a high priority in their work.

Table 3 Diagnosing security-impeding groupthink

1. On a scale from 1 (lowest) to 10 (highest), how high a priority is security for the leader and each member of the team?
2. Do we have explicit criteria to detect and respond to security threats? If yes, identify; if no, explain why not.
3. Does each team member ask questions about security? If yes, how often; if not, explain why not.
4. How do the team leader and other individuals respond to a member who expresses concern about security?
5. What recourse does a team member have if the leader and/or other members shun a person who expresses concern over an imminent or potential security threat?
6. How many objections has each team member heard about security? What did they do in response?
7. How many outside experts have been invited to inform and instruct the team on security prevention measures and real-time response tactics?
8. Does the leader designate special or additional meetings for potential or actual security breaches?
9. What is the team willing to give up to increase security? What is the organization willing to give up?

5.2. Do we have explicit criteria to detect and respond to security threats?

A CIO/PriceWaterhouseCoopers survey of best practice security groups found they suffered over one-third more security incidents, but less downtime and fewer financial losses (Berinato & Ware, 2004). This finding suggests that technology groups give more attention to solving efficiency and cost problems than detecting and eliminating security problems. From our work with technology teams, we question if most programmers would know how to respond to a serious impending security breach. The presence of crisis management techniques within and across organizational units with regard to security is more a rarity than a staple. Including groupthink awareness scenarios and team level follow-up preventive methods in routine training (with accompanying technology prevention capabilities) should be a first step.

5.3. Does each team member ask questions about security?

Until all technical and business team leaders and members make professional commitments to de-

tect and prevent security threats, companies are at risk. A common complaint from technology group members is that meetings are often infrequent, and are mostly oriented toward putting out fires and problems members cannot solve individually. Cross-functional meetings called to inform groups of and orient groups to business performance updates and new initiatives rarely have security on the agenda, unless there is a specific problem or issue (e.g., virus, need for protective software, etc.). Team members must be trained and oriented to identify and manage groupthink symptoms and be knowledgeable about specific security technologies to prevent electronic crises.

5.4. How do the team leader and other individuals respond to a member who expresses concern about security?

Technical team leaders who do not actively create and support critical thinking and open expression of security threats are already susceptible to groupthink; consequently, the organization's security is at risk. In this instance, Janis's recommendations for overcoming groupthink (see Table 2) are relevant and should be instituted as part of a technical team's recurring training. In this regard, the board, CEO, and CIO can play key roles in setting policy to ensure this training takes place and is overseen by senior managers, to whom team leaders report.

5.5. What recourse does a member have if the leader and/or other members shun a person who expresses concern over imminent or potential security threats?

Ideally, a responsible and responsive team leader should provide a "safe" environment in which disagreeing members can comfortably voice security threats. When this is not the case, however, the company board, CEO, and CIO can step up to the plate and provide due process procedures for lower level team members. There are many disconnects between board level concerns about security, CEO strategy, and CIO operating policy as these filter down to technology group procedures. Pressures to conform, self-censure, and conceal or deny security problems reinforce the need for due process procedures by which even technical team leaders must abide.

Corporate and government policies to improve security do not necessarily lead to organizational cultures that encourage raising security issues. Unfortunately, many closed organizational and team cultures force conscientious members to self-censor, do nothing, or blow the whistle, which often results in retribution against the "offender". The United States Computer Fraud and Abuse Act has been used to prosecute whistleblowers. Bret McDanel served 16 months in jail for publicizing a security hole in his former employer's e-mail product after becoming dissatisfied with how long the company took to address the issue (Krause, 2005). A regular target of hackers' and defensive software vendors' animosity is Steve Gibson, whose "Shields Up" website (https://www.grc.com/x/ne.dll?bh0bkyd2) provides information on Internet security breaches and tools to deal with them. To build a culture of security, whistleblowers must feel safe. This requires a management ethos that supports and even encourages those who advocate for security and point out weaknesses.

5.6. How many security objections has each team member heard? What did they do in response?

The CIO/PriceWaterhouseCoopers survey found that in over half of security incidents, no one was notified (Berinato & Ware, 2004). CIOs should frequent technical team meetings to observe cultural and communication dynamics of participants and team leaders. CIOs can also use the devil's advocate method to assess each team's alertness and attention to security threats and prevention. Notes from team meetings should be transcribed and become part of a company's record; access to such notes clarifies to all members that objections to security threats must be justified. CEO, CIO, and board policy are necessary with regard to this suggestion.

5.7. How many outside experts have been invited to inform and instruct the team on security prevention measures and real-time response tactics?

Even large organizations have difficulty keeping up with the latest advances in security. Many mid-sized organizations we study view security as either a technical problem that needs "fixing" or as a policy concern that requires some attention. Using outside experts to glean best organizational and team practices in preventing and managing security can motivate, inform, and commit officers and team leaders to integrate security throughout the firm as a high priority.

5.8. Does the leader designate special or additional meetings for potential or actual security breaches?

As reflected by the infrequency of breach reporting and the shunning of whistleblowers, there is a tendency to deemphasize negative events. The more attention paid to security, the more likely the organization will take the issue seriously and move beyond groupthink. A major barrier group level leaders face is having to "fight the system to protect it", as one professional told us. Again, we argue electronic security will remain simply a "good idea" until and unless enterprise policy at the board, CEO, and CIO levels are translated into operating and due process procedures technology team leaders and members must use. Translating groupthink symptoms into technology leadership and group awareness practices is a logical starting point.

5.9. What are the team and the organization willing to give up to increase security?

Many groups and organizations find it easy to claim security is a priority until they are faced with difficult choices. If an organization made explicit that either deadlines or functionality would have to be sacrificed to ensure security, it would lend the issue the gravity it merits. Technology and business teams could also benefit from using case studies of crises, including the Y2K debacle, as training methods. Many younger technology team members have little to no memory of Y2K or any other corporate crisis, save Enron and a few other recent company scandals. Emphasizing the seriousness of potential security crises and accompanying costs is not a widely used training method for technology teams. If companies value their reputations and respect their customers, stakeholders, and employees, they might ask themselves more often what they are willing to give up to prevent security crises.

6. Final thoughts

From company officers to systems developers, business and IS professionals may be repeating errors in their security systems similar to those that led to Y2K. Worldwide, Y2K remediation cost hundreds of billions of dollars. If that crisis was not a sufficient warning, what will it take now? Had Y2K led to catastrophic failures rather than massive expenditures, perhaps more effort would have been expended toward learning from those mistakes. The 9/11 crisis should have been another wake-up call for security in general, but information security is still not a strategic or operational priority in most organizations.

Information systems research and organizations have focused heavily on aligning IS and business. As noted previously, IS has become so focused on alignment that it has lost the drive to dispel groupthink. Being part of the "team" and "speaking the same language" have become paramount. Just as early Y2K warnings were ignored, so too have been warnings regarding security. Boards of directors, CEOs, CIOs, and other company officers must enact, institutionalize, and monitor policies and procedures that support and enforce security prevention practices. However, unless IT leaders and professionals are able to identify the symptoms of groupthink as security problems and address them directly, further failures are inevitable, with serious consequences likely to occur.

References

Anderson, J. E., & Schwager, P. H. (2002). Security in the information systems curriculum: Identification and status of relevant issues. *Journal of Computer Information Systems*, *42*(3), 16.

Austin, R. D., & Darby, C. A. R. (2003). The myth of secure computing. *Harvard Business Review*, *81*(6), 120–126.

Bartels, A. (2004). *Projected 2004 IT spending growth: Inching upward*. Cambridge, MA: Forrester Research.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, *25*(4), 375–414.

Berinato, S., & Ware, L. C. (2003). The state of information security 2003. *CIO*, *17*(2), 1.

Berinato, S., & Ware, L. C. (2004). Global security survey '04. *CIO*, *17*(23), 1.

Capretz, L. F. (2003). Personality types in software engineering. *International Journal of Human-Computer Studies*, *58*(2), 207–214.

CSC Index Research and Advisory Services. (1997). *The year 2000 problem (No. 111)*. London: CSC Index Research and Advisory Services.

Cutter Consortium. (2001, May 17). *For e-projects, do it right and deliver on time*. Retrieved May 31, 2002, from http://www.cutter.com/press/010517.html

Deloitte Global Financial Services Industry. (2004). *2004 global security survey*. Retrieved from http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_SecuritySurvey2004_051704.pdf

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67–87.

Ernst, & Young. (2004). Global information security survey 2004. Retrieved from http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf

Glaser, J. (2005). More on management's role in IT project failures. *Healthcare Financial Management*, *59*(1), 82–84.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). 2004 CSI/FBI computer crime and security survey. Computer security institute. Retrieved from http://www.reddshell.com/docs/csi_fbi_2004.pdf

Hofmeyr, S. (2003). Why today's security technologies are so inadequate: History, implications and new approaches. *Information Systems Security, 12*(1), 17–21.

Information Technology Association of America. (2003). *Report of the ITAA blue ribbon panel on IT diversity*. Arlington, VA: Information Technology Association of America.

Janis, I. L. (1983). *Groupthink* (2nd ed.). Boston: Houghton Mifflin Company.

Koetzle, L. (2003). *How much security is enough?* Cambridge, MA: Forrester Research, Inc.

Krause, J. (2005, February). Computing time for the crime. *ABA Journal*, *91*, 14.

Lohmeyer, D. F., McCrory, J., & Pogreb, S. (2002). Managing information security. (Special Edition). *McKinsey Quarterly, vol. 2* (pp. 12–16).

McAdams, A. C. (2004). Security and risk management: A fundamental business issue. *Information Management Journal*, *38*(4), 36–44.

Mercuri, R. T. (2003). Standards insecurity. *Communications of the ACM*, *46*(12), 21–25.

OECD. (2002). OECD guidelines for the security of information systems and networks: Towards a culture of security. Paris: Organisation for Economic Co-Operation and Development.

Paulson, L. D. (2002). Post 9-11 security: Few changes, business as usual rules. *IT Professional*, *4*(4), 10–13.

Peck, W. G. (2003, October 13). An evolving job description. *Journal of Commerce*, 1.

Penn, J. (2004). IT spending continues to focus on security. Cambridge, MA: Forrester Research.

Power, R. (2003). 2003 global security survey. New York: Deloitte Touche Tohmatsu.

Pressman, R. S. (2000). What a tangled Web we weave. *IEEE Software*, *17*(1), 18–21.

Sanders, J. (1998). Y2K: Don't play it again, Sam. *IEEE Software*, *15*(3), 100–102.

Schein, E. H. (1996). Three cultures of management: The key to organizational learning. *Sloan Management Review, 38*(1), 9–20.

Surmacz, J. (2004, March 16). *Test of loyalty. CIO.* Retrieved from http://www2.cio.com/metrics/2004/metric673.html

Tapia, A. H. (2003). Technomillennialism: A subcultural response to the technological threat of Y2K. *Science, Technology, and Human Values*, *28*(4), 483–512.

Thomsett, R. (1998). The year 2000 bug: A forgotten lesson. *IEEE Software*, *15*(4), 91–95.

Williams, R. D., & Smyth, B. T. (1999). Historical development of the Y2K problem: Challenging the conventional wisdom, part III of III. *Computer and Internet Lawyer*, *16*(4), 10–20.

Yardeni, D. E. (2005). *CIO magazine tech poll*. CIO Retrieved from http://www2.cio.com/techpoll/index.cfm