Creating a Culture of Enterprise Cybersecurity

Allen W. Batteau
Wayne State University

In this article I describe the fundamental dimensions of a security culture, a concept that builds on the experience of "safety culture" in several high-hazard industries. After outlining the concept and subtleties of corporate culture, I apply these concepts to issues of security, focusing on issues of trust, identification and authentication in complex environments. These issues become more challenging in virtual environments, as familiar tokens of identity such as face-to-face recognition are absent, and where trust becomes a weakest-link problem. I conclude with a description of the challenges of "managing" the emergent phenomenon of culture, and how trust can be cultivated.

INTRODUCTION

Cybersecurity – the protection of computer networks – has become a major concern of businesses and governments. As networks extend our ability to communicate widely, they expose us to hackers, business competitors, disgruntled co-workers, and other predators with vandalistic or larcenous intent. It is only a matter of time before some terrorist somewhere hacks a poorly protected public safety network in some small town, causing major property damage or loss of life.

When computers were standalone devices, security was a minimal concern. Mainframes had their own protected facilities. As computing became more personal, security, too, became a personal responsibility: if you transferred a file using a floppy disk, you first scanned the disk for viruses. As the use of computers increasingly involves networks of computers, whether for messaging, conducting on-line transactions, or remote hosting, the opportunities for attack have multiplied exponentially: data from the Electronic Security Alliance indicate that security incidents have doubled every year, a perverse acceleration of Moore's law.

In America, the land of the techno-fix, discussions of cybersecurity overwhelmingly focus on hardware and software: encryption algorithms, firewalls, electromagnetic emissions, biometrics, retinal scans, and other devices to shield systems from unauthorized users or spectators. As important as these are, they are only one-third of the security equation, and a too-exclusive focus on the technology of security, as Bruce Schneier argues in *Beyond Fear* can actually leave institutions more vulnerable to security gaps (Schneier, 2003). The September 11, 2001 hijackers combined high-imagination strategy with low-tech methods, relying on gaps in visa regulations and airport screening to accomplish their terrible purposes. For the defenders of America, these attacks, as the September 11 Commission reported, represented a "failure of the imagination." (National Commission, 2004)

The other two-thirds of the security equation beyond technology are *people,* and *process*. Any security manager who is not attending to people, process, *and* technology is inviting a major, and perhaps disastrous incident.

In this article I describe some strategies some strategies for approaching the first of these terms, *people*. I describe them from the standpoint of a cultural anthropologist who has worked in IT and observed corporate cultures in business, government, and military environments for more than 20 years. My data come from specific projects in enterprise integration, operational safety, and homeland security, in which my team collected data on the significance of culture and identity for enterprise effectiveness and operational integrity in these arenas. Our research examined "people" primarily in terms of organizations and organizational cultures, group-level issues that are a separate matter from the individual-oriented focus of "human factors." "People" is about both groups and individuals, two separate though related problems. At the individual level, such issues as training and selection, and motor and cognitive skills and aptitudes, are paramount. At the group level, which we are concerned with here, shared values and commitments – culture, in short – has a strong, if poorly-understood determinant of organizational performance.

To describe these group-level challenges I will first describe what culture is and why it is important for businesses and institutions. I will then describe the characteristics of a security culture, building on the well-developed understanding of safety culture in aviation and other industries (Antonsen, 2009; Pidgeon, 1991). I will then describe the unique challenges posed for these in on-line transactions, where relationships are often anonymous, and where determining where and how to draw the boundaries of trust is a rarefied and abstract effort. "People" means one thing in a face-to-face group, and something quite different in a chat room or other electronic meeting place.

These unique challenges are multiplied in today's emerging organizational form, the networked enterprise. Whether found in a product collaboration or a manufacturing supply chain, networked enterprises integrate nominally independent corporations and producers, each having its own security policies and procedures, its own corporate culture, and its own unique business strategy. In these enterprises, cybersecurity is a weakest-link problem, and the company that is unable or unwilling to maintain appropriate security standards either drops out, is shut out, or damages the entire network. Conversely, tightly coupled networks that are unable to agree on and enforce a common set of security standards and policies must degrade, either gracefully as when they decide "we cannot be so tightly linked", or catastrophically as from a massive virus attack. I will conclude by describing some of the strategies through which a security culture can be built and tailored to an enterprise's business objectives.

CORPORATE CULTURE

"Corporate culture" quickly made the transit from an academic theory to a consultants' nostrum, pausing only in a few places to take root as a serious management strategy. Where it has taken root, in companies such as Motorola and Southwest Airlines (both of which include culture as part of their senior executives concerns), it has produced a committed workforce and a coherent business strategy. In other companies (which shall not be named here), in the absence of leadership vision, local cultures have sprung up like weeds, creating numerous patches of resistance to corporate objectives, optimized for their own purposes, yet and draining off resources toward non-strategic ends.

When one asks companies with a coherent corporate culture about their culture, time and again the phrase "the way we do things around here" comes up. Although this phrase sounds fairly bland, it actually has great meaning for those who use it. For them, their culture is first of all that which is typical ("the way") for their company, and acting on it ("we do things around here") has a totemic status for them and their company: it establishes their identity. When this sense of identity and ownership is especially strong it guides behavior far more effectively than any management directives or supervision. Employees give 110% or more because it is *their* company, not some remote shareholders'.

A corporate culture is an informal order, existing alongside the formal order of the corporation, commenting on, reinforcing, or critiquing the formal order. Every formal rule in a corporation has an informal commentary: When a new directive is issued from the executive suite, those below negotiate and quickly figure out whether it is "flavor of the month" or "they really mean it this time." Existing policies are parsed as to whether they are mission-critical or simply window-dressing. These negotiations take place in the social spaces of the corporation, and astute leaders attempt to harness them rather than suppress them.

Although the association between culture (in this nuanced sense) and performance is intuitively obvious, numerous studies have attempted to find, so far with disappointing results, correlations between measurements of corporate culture and performance. The disappointment is the result of a too-narrow understanding of both culture and performance, focusing only on that which can be quantified. The *quality* of relationships, an irreducible complexity, is often more important than the quantitative measurement of attitudes. Eastern Airlines, for example, had a strong culture of labor-management hostility. Each side dug in its heels and took the position that rather than give in to those other guys, they preferred to see the company go under. It did. Other examples, usually less extreme than this, make it clear that when a corporation's culture embraces antagonism between employees and management *from either side*, it degrades performance, or more accurately, diverts performance in less than optimal directions. On the employee side, in some manufacturing firms one finds a culture of "homers," home-built items, sometimes quite elaborate, assembled with care using parts and tools pilfered from shop inventories. On the management side, compensation uncoupled from or disproportionate to a firm's well-being is an executive "homer." Both are equally poisonous to the company's culture.

In contrast to cheerleading and superficial views of corporate culture (Batteau, forthcoming), a critical view of organizational culture recognizes that it consists of an interplay of cultures of command, cultures of accommodation and resistance, and cultures of inclusion and alienation, all within a framework of instrumental rationality (Batteau, 2011). Each of these interacts with and interrogates the others: Employees can resist management directives by taking them seriously ("malicious compliance," or "work-to-rule" strategies). Managers can appeal to shared sentiments, or they can alienate their workforce with heavy-handed directives or blatant insincerity.

A corporate culture is always contingent and emergent, and can never truly be managed. Corporations bring together numerous groups – their workforce, their professionals, their managers, their suppliers, and their customers – in more or less permanent relationships. When the relationships are more permanent, shared understandings and trust can grow up among them, which then reinforce the permanence of the relationship. If any one group attempts to assert itself in this mix to too great an extent, it engenders resistance; shared understandings then become a mutual “we (labor, management, customers, and suppliers) had better take advantage of you before you take advantage of us.” A culture of “negative reciprocity” (Sahlins, 1972) thus becomes firmly established.

At their best, these shared understandings create high levels of trust among members of a company. Communication becomes efficient and deep: parties have a sufficient depth of shared experience and understanding that a few words can evoke complex thoughts. It is this corporate landscape, this refinement of trust – that supports a strong security culture.

SECURITY CULTURE

Commercial aviation is without question the safest form of transportation available. This is due, in part, to a strong safety culture shared by flight crews and executives alike, which includes thorough training, adherence to procedures, and an uncompromising acceptance of safety standards: Pilots accept, unhesitatingly, the directives of air traffic controllers because they know that those directives are all that stands between them and the other airplanes in their airspace. The high level of trust among pilots, controllers, and mechanics is probably without equal in any other industry.

A group of political scientists, engineers, and management theorists at University of California Berkeley have studied organizations that they characterize as “high reliability organizations,” (Roberts, 1990; Roberts and Rousseau, 1989), a concept that has been closely linked to safety culture (Pidgeon, 1991). These include nuclear power plants, naval aircraft carriers, and air traffic control centers. Among the features shared by these organizations are constant training mode, accountability pushed to the lowest level, reliance on open and robust communications, and shared perceptions of hazards. Constant training mode assures continued vigilance; accountability pushed to the lowest levels empowers all hands to take action to ensure safety; redundant personnel assures “multiple eyes” on hazardous operations. The environments in which these observations were made were all spatially restricted, and not open to competitive pressures, and probably not replicable in the competitive world of business.

Like safety culture, security culture is part mind-set, part nuance, part social connection. Should it be the responsibility of individual employees, or of tech support, to keep anti-virus software up to date? This depends on the resources available, the nature of the company’s business, and the potential loss from a catastrophic attack. Should employees simply delete infected email attachments, or inform a security officer? Again, it depends on the company’s security policy.

Like safety, security is also a matter of nuance. A good safety culture does not mean that the crews are excessively cautious, but rather that they are prudent and well-informed. With years of experience pilots develop a strong sense of their flying abilities, how far they can push on in adverse conditions, and when they should divert to an alternative destination. In similar fashion, security culture is not the same as paranoia. Security managers have to make judgments on the tradeoffs among reach, openness, and ease-of-use of information. What forms of identification and authentication do we require before we let which users into which levels of our system? The paranoid answer, “trust no one,” reveals a deficit of thinking. We always *do* trust some people, once they have been properly identified and authenticated. So what is the basis of that trust? Because they are employees? Most network attacks come from inside the company. Do we trust people because they have promised never, ever to download questionable material from the world wide web? Do we trust someone because he is our cousin? Our best friend from school?

These are questions a security policy must answer; equally important, anyone who has access to an enterprise network must be familiar with the policy. Management support for the policy is equally critical.

Equally significant as the bases of trust are the methods of identification and authentication, and the training and supervision of employees in these. Is an employee badge required to get into the building and get on the network? If so, how strictly do we enforce badge rules? Working as a consultant, I took (perverse, to be sure) enjoyment in observing how some well-known companies were only going through the motions of security by allowing secured doors to close slowly (thus permitting me to follow a trusted employee into the building), by waving in familiar faces even without badges, and by exchanging ID tags and passwords. In many companies, these are firing offenses; some of them actually mean it. In more companies, they simply go through the motions. These companies have made a decision that the costs of intensive training and supervision are greater than they can justify; the hidden costs in employee cynicism of such skimping security, are not accounted.

Software can be hacked. Hardware can be bypassed. Policies can be weakly enforced. Trust can be abused. In other words, there is no single, foolproof security measure. The only silver bullet for security is to weld the doors shut, disconnect the electric power, fire all employees, and go out of business. Short of these drastic measures effective security measures always include *defense in depth*, and *people in the loop*.

Defense in depth is the opposite of the techno-fix. It means having multiple (and consistent) policies, procedures, and resources reinforcing security, so that if one is breached, another backs it up. It requires an in-depth understanding of the company's business (more so than any consultant is likely to have), and a requisite imagination to anticipate a variety of threats: it is the opposite of the "trust no one".

"People in the loop", of course, begs the question of "which people." Bruce Schneier makes it clear that often people are the last and most resourceful line of defense: It was the passengers, not the US Air Force, that saved the White House from the hijackers on American Airlines 87 on September 11, 2001. It is the trained and experienced police officer or customs agent that spot the suspicious passenger or package, as much as the screening machinery.

For more ordinary situations, perhaps the greatest task of security culture is deciding which people to trust, and why. Categories of identity (my cousin, my fraternity brother, my boss, those guys in accounting) are no substitute for training and shared experience, reinforced by long-standing and multi-stranded relationships. Ironically, as the importance of enterprise security increases, pressures for downsizing, described in Karen Ho's book *Liquidated*, (2008) undercut the greatest resource for this security.

Within a strong safety culture, open communication is an essential element. When errors and mishaps occur, they are discussed openly, perhaps even posted on on-line bulletin boards. Those who report them are not punished, but rather congratulated for helping everyone else learn. Could this be applied to breaches of security? Most security personnel, trained in a tradition emphasizing suspicion, would react in horror at the idea of posting information on every slip-up in baggage screening or firewall protection.

In fact, however, slip-ups happen, and that they do not happen more often is a major vulnerability. Among computer security professionals there is open discussion of incidents, from which all learn how to further protect their systems. When incidents are covered up, by contrast, it assures that they will be repeated. In other fields such as transportation security, where more of a police state mentality prevails, security breaches continue because there is no open discussion from which all can learn.

One could model the consequences of systems where security breaches are revealed or concealed. If the majority of airline passengers are potential terrorists, then extreme secrecy about security would make great sense. On the other hand, if the majority of airline passengers are potentially vigilant citizens, - such as the fellow-passengers who restrained the "underwear bomber" on Northwest 253 in December, 2009 -, then open discussion would have the consequence of increasing vigilance. Unfortunately, from the airlines' point of view, it would also make honest citizens more reluctant to fly.

The key element is that such discussions must take place within a context of trust and respect. Again, figuring out whom to trust, and communicating respect, is a major challenge. As enterprises evolve from top-down command-and-control hierarchies into networks of collaboration (Heckshер and Adler, 2006) answering this question will graduate from a maintenance issue into a core part of business strategy, as it has for the one area of intellectual property protection.

"PEOPLE" ON-LINE?

As difficult as this is in our everyday, face-to-face lives, its complexity grows in on-line or computer-mediated communication. When business was conducted with a close circle of nearby associates, this was easy. More distant commercial relationships were often handled through trusted intermediaries, such as banks, in which both parties placed their trust (and their funds). These fiduciary institutions were trusted in part because of the social prestige of their owners and officers, and in part because they are in a highly regulated environment.

In today's business environment these relationships have broken down. Relationships are numerous and distant; leading institutions have sometimes show themselves unworthy of trust (think Arthur Andersen, or Lehman Brothers, or Countrywide); mortgage lenders have evolved from pillar to predator in many communities. In this brave new world, we trust sensitive information and funds to people we have never met, defining a circle of trusted associates is nearly impossible.

Progress can be made in understanding different forms of online communication, and in developing clearly understood bases for trust. These would not necessarily be as formal or rigid as the schemes of security clearances in the military; our research found that concerns about security breaches in certain Air Force components sometimes impeded activities (such as on-line exchange of engineering data) that would be considered normal business elsewhere. Part of the problem was that a set of rigid security rules had been devised for an environment of paper documents, and had not been updated as more transactions went online.

Communication on line ranges from personal to impersonal, and security measures range from hard (such as highly restrictive firewalls) to soft (such as user authentication and passwords). Some transactions are confined to a relatively small and permanent small circle, whereas others must take place in amorphous and flexible networks. An example of the former might be the information that goes into a company's financial reporting, whereas the latter would include most retail transactions and design collaborations. A company's security architecture (the articulation of hard and soft defenses and policies and procedures) can be monolithic and Stalinoid, one-policy-fits-every-transaction, or it can be resilient and nuanced. Understanding that the same security policies and technologies are not appropriate for both of these is an important part of security culture.

For a few companies (most notably financial institutions and protective agencies), security has always been a core part of their business strategy. There was a time when securing the vault was at the core of banking, and banks advertised their vaults' impregnability. Physical solidity was a brand identity. Although there are fewer concerns today with physical predators, the rise of cyberpredators requires a new attitude toward security. For businesses that rely on on-line transactions, developing a reputation for information security, as PayPal has done, is a core part of their business strategy.

The security policy of these enterprises will include recognition that different forms of on-line transaction have different vulnerabilities and different security requirements. Thus (for one of many potential examples) a company could have a relatively open e-mail system with messages being screened to assure that they are not conveying company data, and a more hardened system for more sensitive transactions. Or employees could be encouraged to participate in industry forums with a clear understanding in advance of what topics were impermissible in those forums. In the on-line world managers need to understand the different ways in which computers can mediate communication, and the different opportunities and threats that each of those carries.

THE WEAKEST LINK IN THE SUPPLY CHAIN

As difficult as network security is for a standalone company, it is even more so for networked enterprises such as supply chains, retail distribution networks, joint ventures, and project collaborations. These networks range from loosely coupled networks where communication is through e-mail and telephone, to tightly coupled networks where one company's systems directly interface with another. An example of this latter would be supply chains where the material release systems and broadcasts of manufacturers send data directly to the order management or material management or shipping systems of their suppliers. The suppliers also respond with online transactions (such as an Advance Ship Notice – sort of an electronic handshake) that feed directly into their customers systems. Electronic Data Interchange transactions such as these are simple, routine, guided by industry standards (ANSI X.12, for example), and are easy to secure with appropriate hardware and procedures. In more complex environments, it is more difficult.

When the relationships are stable and when there is one dominant player in the chain, common security policies and procedures can be enforced by the dominant player. This roughly describes the Japanese *keiretsu*, or family of companies, where suppliers follow the lead of their Original Equipment Manufacturer (OEM) "parent". *Keiretsus* are a modified form of the familiar top-down hierarchic enterprise, and recent experience has suggested that this is an inflexibility.

We can expect that the security policies and practices of networked enterprises will evolve to a stable state that is supported by their resources and their culture. Along the way some members of the enterprise will drop out or be pushed out. Security levels will rise (or fall) to the point that works best. An enterprise of highly committed employees, all other things being equal, will have a higher level of security than one full of angry, insecure employees and disgruntled suppliers; an enterprise rich in knowledge resources likewise will be able to support higher levels of security than one of widespread ignorance regarding security threats and requirements. This suggests that widespread and recurrent training in security strategies, policies, and procedures may be more critical than purchase of surveillance or authentication equipment, as suggested by High Reliability Theory. Yet far too frequently, one observes in the corporate and military world that the purchase and installation of whiz-bang hardware gets more attention than boring training. This, too, is a security culture, or perhaps more accurately a vulnerability culture.

CAN CULTURE BE MANAGED?

Companies are not machines, and their employees, suppliers, and customers are not mechanical components. Nevertheless, the mechanistic ideal where everything hums along "like clockwork" is an ideal that many managers aspire to. This mechanistic ideal thoroughly ingrained in American business. Despite a complete absence of advocates for raw Taylorism, Tayloristic management is still quite common: For example, the 1980s movement for "re-engineering" was little more than Taylorism applied to administrative processes.

Homo Sapiens has spent approximately 100,000 years – 5000 generations – learning a form of adaptation in which small, face-to-face bands foraged in an unforgiving environment through calibrated adjustments of cooperation and competition with neighboring bands. Sometimes they would fight, sometimes they would intermarry, sometimes they would hunt together, and many times these three activities were not clearly distinguishable. There has been ample evolutionary time for a certain form of relatedness and adaptation – optimal foraging in bands, trust based on face-to-face cooperation, and alliances built on trusted adversaries – to become hardwired into our DNA. This still works, as many entrepreneurs can attest. Even today, despite the ubiquity of networked communications, entrepreneurial clusters, whether in Silicon Valley or Mumbai rely on face-to-face communication.

Part of this adaptive repertoire is a propensity to favor learned response patterns over instinct, and through social sharing to build repositories of generational learning. "Culture" is another name for these repositories of knowledge, tuned to a specific social and physical environment.

One of the requirements of cultural adaptation is that behavior makes sense. Cultural response represents a higher level of learning than the stimulus-response training of laboratory animals. Although *homo sapiens* do respond to reinforcements, it is always for low-level behaviors: No combination of rewards and punishments can ever produce a symphony or a great business plan. Humans are not lab rats.

This makes cultural "management" far more challenging. When humans are treated as cogs in a machine, they return the favor by exhibiting all the learning capability of spur gears. Entire industries have ground to a halt because they tried to suppress the learning capability of their members. More prosaically, numerous industries perform sub-optimally because they fail to take advantage of the intelligence and resourcefulness of the people within them.

Cultures cannot be managed – at least not with "management" in a conventional sense – but groups can be led, and if allowed spaces for growth, can evolve cultures. Leaders cannot dictate a culture, but they can create goals and symbolic ideals toward which cultures can evolve. Leaders can present examples of integrity, and the spaces for employees and clients and customers to observe, try on, and imitate those examples.

Most of the literature on "corporate culture" can be divided into three different types of effort. The first type is the useful effort of making managers aware that culture exists, and that in their organizations they are sitting on top of living, breathing cultures that may or may not conform to the managers' quarterly objectives. In these efforts at cultural sensitizing, managers are treated as intelligent beings who, once aware of an issue, can adapt.

The second type of effort builds on this, describing and analyzing these cultures, whether in terms of stories, myths, rituals, heroes, behavior patterns, all in varying combinations (Rosen, 1985; or Van Maanen, 1991, for example). This is also useful, in that it opens a storehouse of knowledge of different cultural forms; a "culture of culture," one might say. The stories about a legendary CEO or a legendary security guard are statements of corporate values. (A frequently told story in IBM is of a security guard who demanded to see Thomas Watson's badge before allowing him to enter an IBM facility. Although Watson's entourage was aghast, Watson backed up the security guard and sent an underling to fetch his badge. The message this story sends to everyone is unmistakable.)

The third type, which is more pernicious, is a substantial body of consultant literature that suggests that an attentive manager can change his culture if he simply manipulates his personnel policies, or his reward system, or his corporate communication, or the corporate dress code, or the office furniture, in some appropriate manner. This literature points to companies that go through "cultural changes", including (as an extreme example) one company that "changed" its "culture" three times in ten years. This view of culture as packaged and commodified sends messages of manipulation throughout an organization.

In line with Americans' desire for quick fixes, in which wealth and happiness are only one self-help book or one motivational speaker away, this packaged culture peddles only cynicism. To avoid the trap of purveying one more quick fix, I will conclude this discussion not with a homily on changing culture, but with an observation that all of the attributes of outstanding leadership - integrity, knowledge, wisdom, communication - are part of fostering a culture that reinforces, rather than undermines strategic objectives. Part of effective leadership lies in the recognition that while culture can further motivation and morale, it also – invariably – creates blind spots that can be overcome only with what Ron Westrum calls "requisite imagination." (Westrum, 1993). A leader must be able to see where others cannot. The wise leader will surround herself with people who can see that which she cannot.

America's contemporary security culture has several blind spots: These include a fascination with techno-fixes rather than balancing trust and mistrust, and a desire for immediate results and a short attention span. Technology, near-term results, and a healthy level of suspicion will always be important; however, an effective security culture will be that which understands that these must be tempered with people-centeredness, patience, and respect. With a defense-in-depth strategy, people are the last and most effective line of defense.

STRATEGIES FOR TRUST IN COMPLEX ENVIRONMENTS

Trust – confidence in another's actions and intentions – has multiple foundations and dimensions. It can be based on shared background, shared experience, a commonality of identity, or a shared understanding of the rules of the game. Trust can be limited to certain domains where one is confident of the other's competence, or it can be extended into unknown territory because one trusts the prudence of the other.

Trust can be generalized or transactional. Transactional trust is tit-for-tat: I will trust you in this transaction because you probably won't gain too much by cheating me. Typically, transactional trust has institutional foundations, whether in the legal code or fiduciary institutions.

Generalized trust is indicative of a strong *social* bond that is not reducible to legal formulations or corporate procedures. It has a flexibility and an adaptability that transactional trust lacks. It can be spontaneous, as happens with two individuals coming together in an extreme situation. Trust can be built up over generations, as in the example of family alliances in business and government. Trust can be reinforced by demonstrations of irrational beyond-the-call-of-duty commitment, or it can be dissolved - “liquidated,” in Karen Ho’s characterization - by corporate downsizings.

In between generalized trust and transactional trust is strategic trust, a nuanced and articulate understanding of whom to trust with which information in which situation. A culture of cybersecurity is a complex amalgamation of generalized and transactional and strategic trust relationships. This culture cannot be designed, in the sense that an engineer designs a complex piece of machinery, but it can be cultivated, in the sense that a gardener cultivates a flower garden.

Learning in such an environment, like the development of any relationship, is a matter of mutual adaptation: it may grow quickly or slowly, and its limits are unknown until they are experienced. A resilient security culture is one that creates opportunities for this learning within clearly defined boundaries. Such learning opportunities range from training exercises to after-action analyses of security breaches.

Paradoxically, the frequent turnover of personnel in institutions such as the military creates perhaps the greatest opportunity for fostering safety cultures. As one informant told the High Reliability researchers, “you’re either in training, or training your replacement.” The fact of training heightens attention, so one is far less likely to get careless when she is in training or training her replacement. This frequent turnover, however, is not the same as job insecurity or downsizings, but is rather a function of duty rotations that are a standard expectation. The sequel of training one’s replacement is, of course, confidence in the next assignment.

This fact, and two others drawn from High Reliability Organizations, form the core of a security culture. Redundant personnel or “multiple eyes” means that errors are more likely to get trapped before they escalate into accidents. In the open environment of an air traffic control tower or aircraft carrier flight deck, there are many eyes watching what the controller or the deckhand is doing, and all have the authority to intervene if an error is spotted. Perversely, the paranoid, secretive aspect of many security environments assures that a careless or determined leaker or hacker can carry on for weeks before being detected.

The second aspect of High Reliability Organizations that would form a foundation of a culture of enterprise cybersecurity would be clearly agreed upon goals, from top to bottom. On the flight deck, shared commitment to safety means that all personnel, from the captain down to the deckhands, participate in making sure that operations are safe.

By contrast, if one aspect of the organizational culture is a culture of alienation, or if there is cynical disillusionment regarding the organization’s integrity, then the only issues in a security breach are “how soon?” and “how massive?” The greatest breach of enterprise cybersecurity in recent years, resulting in the Wikileaks disclosures of military and diplomatic activities in Iraq and elsewhere, apparently came not from the outside. Rather this breach allegedly came from a low-level computer operator, PFC Bradley Manning, at a time when there was widespread cynicism and disillusionment, by military and civilians alike, regarding the American mission in Iraq.

A resilient security culture, like the safety culture in High Reliability Organizations, is one face of organizational integrity, in which a strong culture of inclusion - “we’re all in this together” – coexists with a clearly defined and accepted mission and commitment of resources appropriate to strategic objectives. Anything less – untrained and embittered personnel, dishonesty regarding objectives, executive “homers”, blindness to environmental threats -

assures that compromised security will eventually compromise an enterprise's mission, and possibly its existence.

ACKNOWLEDGEMENT

This material is based upon work supported by the National Science Foundation under Grants numbers 0740067, 0519440, and 0428216. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation (NSF).

REFERENCES CITED

Alvesson, Mats. (2002). *Understanding Organizational Culture*. London. Sage.

Alvesson, Mats, and Hugh Wilmott. (1996). *Making Sense of Management.* London. Sage Publications.

Antonsen, Stian. (2009). Safety Culture and the Issue of Power. *Safety Science*, 47, 183-191.

Batteau, Allen. (2000). Negations and Ambiguities in the Cultures of Organization. *American Anthropologis,t* 102, (4), 726-740.

Batteau, Allen (forthcoming). Speaking of Corporate Culture. In Jordan, Ann, and Douglas Caulkins, eds. *Companion to Business Anthropology,* New York. Wiley-Blackwell.

Ho, Karen. (2009). *Liquidated: An Ethnography of Wall Street*. Durham. Duke University Press.

Pidgeon, Nick F. (1991). Safety Culture and Risk Management in Organizations. *Journal of Cross-Cultural Psychology*, 22(1), 129-140.

National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission Report*. New York. W. W. Norton.

Roberts, Karlene. (1990). New Challenges in Organization Research: High Reliability Organizations. *Industrial Crisis Quarterly*, 3, 111-125.

Roberts, Karlene, and Denise M. Rousseau. (1989). Research in Nearly Failure-Free, High-Reliability Organizations: Having the Bubble. *IEEE Transactions on Engineering Management,* 36(2), 132-139.

Rosen, Michael. (1985). Breakfast at Spiro's: Dramaturgy and Dominance. *Journal of Management*, 11(2), 31-48.

Sahlins, Marshall. (1972). *Stone Age Economics.* Chicago. Aldine-Atherton.

Schneier, Bruce. (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York. Copernicus Books.

Van Maanen, John. (1991). The Smile Factory: Work at Disneyland. In Frost, Peter J., Larry F. Moore, Meryl Reis Louis, Craig Lundberg, and Joanne Martin, eds. *Reframing Organizational Culture*. Newbury Park, California. Sage Publications. 58-76.

Westrum, Ron. (1993). Cultures with Requisite Imagination. In Wise, John A., V. David Hopkin, and Paul Stager, eds. *Verification and Validation of Complex Systems: Human Factors Issues.* Berlin. Springer-Verlag. 401-416.