Balanced Design in
Information Systems Security Planning

Daniel A. Stern
University of Denver
1225 17th St #3200, Denver, CO 80202
danielasherstern@gmail.com

ABSTRACT

Information security is traditionally understood to involve technical security measures, such as intrusion prevention systems, to establish a secure perimeter around an organization’s sensitive information. Threats, then, are any potential attack on that secure perimeter with the intent of either obtaining unauthorized access or damaging availability or information. With modern organizations using tools to allow every employee to access information, and even allowing employees to control access restrictions on sensitive information, information security managers must expand their information security program to educate personnel and establish a culture of security. The expanded information systems security program must address technical, policy, standards and norms, education and cultural initiatives.

KEYWORDS

Information security, security policy, information security planning, ISSP, human factor, information security design, security architecture

1 INTRODUCTION

Information is vital to operating a business. Every organization uses personal information about its employees for its business operations and employee collaboration. The business relies on maintaining the confidentiality, integrity and availability of that information to operate privately and effectively [1]. Shortcomings in any of these categories can quickly cause significant impact, such as “infringements of human rights, financial damage to corporations and the failure of the entire information system” [2].

While securing a system from intentional attack is a scientific process with specific requirements and measurable performance [1], guaranteeing user compliance and security-affirming behavior is much more challenging. “No matter how well designed, security methods rely on individuals to implement and use them” [3]. Sensitive information is handled by most, if not all, employees in an organization. Every employee must comply with policies and processes, act carefully with information and be prepared to make decisions when facing new risks.

Even respected information security techniques involving compliance and audit may fail to address real contemporary information risk. “Traditional approaches to information security, such as publishing a thick manual of policies and standards, no longer work. They might be fine for enabling you, and your management, to tick your compliance boxes, to demonstrate that you’re discharging your corporate responsibilities. But lengthy edicts are ineffective as a means of influencing staff” [4]. While detailed policies and standards may have been effective when technical users were all experts with such documentation and they were the only ones with access to sensitive information, they are not effective now.

2 GROWTH AND TRENDS IN INFORMATION

Information systems use continues to grow worldwide. In 2012, 34% of households
worldwide had internet access and six billion people used a mobile phone or tablet [3]. Gartner [5] predicted that by 2014, two billion computers would be installed and the International Telecommunication Union [6] reported that number has already been exceeded. In the United States, more than 75% of households have computers compared to 61.8% in 2003 and just 8.2% in 1984 [7]. Internet access is nearly as widespread with 71.7% of U.S. households having access in 2011 and 48% of adults (15 years old or older) accessing the internet using smartphones [7].

With growing information technology use is faster processing capability and growing electronic information (data) storage. Mark H. Kryder in 1989 predicted by 2000, personal computer (PC) RAM would have a capacity of one gigabyte and PC information storage capacity would need to reach ten gigabytes. “Since the introduction of the disk drive in 1956, the density of information it can record has swelled from a paltry 2,000 bits to 100 billion bits (gigabits), all crowded in the small space of a square inch. That represents a 50-million-fold increase” [8]. While at the time Kryder’s predictions may have appeared lofty, his vision has become reality and information storage has grown far beyond levels realized in 2000.

Smaller and more efficient storage media increases vulnerability to physical attack and makes security more complex and increases risk [9]. While at one time sensitive information may have only been stored on mainframe computers, “the problem is now being compounded as organizations must start paying attention to the small personal computers spreading throughout their organization. The problem, rather than decreasing in complexity, grows more acute as each terminal is added” [5].

Information storage is not the same now as it was even just a few years ago during the shift away from mainframe computers. In addition to small and portable storage, new “cloud” technology offers server-side processing and storage [10], sometimes distributing user data among multiple datacenters. Cloud solutions are especially valuable for long term information storage when the data may not need frequent access. Consistent security of cloud information storage is still somewhat unknown. Few standards exist for cloud storage [11] and most providers offer proprietary applications for access. Although some concepts used in today’s cloud storage are not new, such as the network being the computer [11], cloud storage has exploded and may continue its significant growth for the foreseeable future. John Toigo [11] highlighted the economy as a key driver of cloud solutions. Along with much faster and more secure networks and reduced hardware needs due to virtualization, economies of scale enable storage providers to “use the same pool of storage capacity to meet the needs of many customers and pass along the cost savings” [11].

Cloud file storage and file sharing tools present a convenient option for consumers and businesses to share information and replace slow and limited traditional network drives. It also offers a strong example of how humans can pose a risk to information security, often without their knowledge. Data has also become increasingly “personalized” in the past few years [9]. Employees bring their own mobile devices to work and often transfer company data to those devices, potentially allowing untrained personnel to control proliferation of sensitive information.

Current technology trends, such as mobility, grid computing, and software-as-a-service, are moving the focus of corporate data flows outside of the corporate perimeter. That demands a more outward-looking security perspective. We need to shift our attention away from merely securing our own backyards, towards working together with business colleagues to build community solutions, for an
emerging business environment that is based on open networks and shared services” [4]

While these tools do provide helpful mechanisms for employees to use and share information, they also reduce the organization’s direct control of information and yield more access control decisions to potentially untrained employees [10]. An alarming number of security breaches are being reported. A PWC [9] survey revealed 93% of large organizations and 76% of small businesses had a security breach in the prior year, costing tens to hundreds of thousands of dollars per breach for major breaches. Breaches are frequent and their scope and impact continues to grow as “malicious breaches affected a majority of respondents across all sectors” [9].

3 INFORMATION SYSTEMS SECURITY PLANNING

To secure information, organizations often begin by developing an information systems security policy or an information systems security plan. Such a policy or plan is intended to unabridged and define “who may access what information in what manner; basis on which the access decision is made; maximized sharing versus least privilege; separation of duties; who controls and who owns the information; and authority issues” [1].

The organization’s information technology department supplements its policy by enacting technical security measures to protect the organization’s logical and physical boundaries from unauthorized access or attacks. The policy or plan along with technical security then comprises the organization’s information security program. The policy guides employees “to appropriate or acceptable use” [12] of “all electronic media” in the workplace [13]. Policies are subject to continual change by authorized personnel to stay consistent with new situations and risks. Benson [14] recommended an “if-then-else” model of security planning to aid an organization in preparing for security challenges.

Although the devices and infrastructure we use to consume information have changed, the way we protect that information and the users that depend on it hasn’t. We still rely on perimeter defenses when the reality is that there are no boundaries. We continue to believe that we have control over devices when we don’t. We hope that users adhere to policies, but we’ve lost control over policy enforcement. We defend the enterprise as if it were static, when in reality it’s dynamic. [15]

4 HUMAN ROLES IN INFORMATION SECURITY

Security policies often neglect to address culture and execution. Human factors were reported by the National Institute of Standards and Technology to represent 84% of economic loss attributed to information security breach, with human error accounting for 65% of loss and dishonest and disgruntled employees representing an additional 19% of loss [16]. Infrastructure loss such as physical damage due to flooding or fires, combined with malicious outsiders accounted for only 16% of loss [16]. McCauley-Bell and Crumpton [16] refer to users as “the most dynamic system component.” Sasse, Brostoff and Weirich [17] further highlighted from Kevin Mitnick’s testimony to US Senate Committee that “the human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.”

Although Mitnick’s testimony was more than ten years ago, it is difficult to identify changes in the industry to minimize human risk.
Information Security standards such as ISO/IEC270001, ISO/IEC27002, ISO/IEC27005, ISO/IEC27006, SP800 and the ISF Standard of Good Practice for Information Security provide paths for organizations to optimize their information security program without addressing the human element [18]. ISO/IEC27001 focuses on Information Security Management Systems (ISMS) and the organization’s ability to establish, implement, operate, monitor, review, maintain and improve the ISMS. “ISO 27001 defines the management aspects of Information Security as ‘organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources’” [18]. ISO/IEC27002 offers best practices for the company’s security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, development and maintenance, information security incident management, business continuity management and compliance [19].

Information systems security professionals strive to become a Certified Information Systems Security Professional (CISSP), a credential requiring years of experience and an 80% score on the 250-question CISSP candidate exam. The exam includes questions from ten domains: access control, telecommunications and network security, information security governance and risk management, software development security, cryptography, security architecture and design, operations security, business continuity and disaster recovery planning, legal, regulations, investigations and compliance, and physical (environmental) security [19]. Yet these experienced professionals earn their credential without any verification of ability to craft policies or design security architecture with regard for human behavior.

Before modern information security standards and practices, even prior to mass adoption of confidentiality, integrity and availability as primary goals in the field, industry professionals began assessing information security and the influence of people on maintaining secure systems. “Managers concentrating on hardware and software rather than on personnel as a means of checking computer abuse. ‘But security is, first and last, a people problem’, says Parker” [20]. “management must recognize that the ‘nuts and bolts, bells-alarm-whistles approach to data security is only a ‘band-aid’ approach. The real vulnerability lies in the people who are operating the computers, accessing information, and handling vital data on a daily basis. Only when the ‘people problem’ is fully addressed can a company consider their security program complete” [20]. People control every piece of information stored on any type of electronic storage. While storage technologies evolve over time, people will always control those technologies. The “hard boundaries (geographical, physical and logical) are breaking down and Information Security has to be managed across a network of partnerships, alliances and outsourcing relationships” [18].

5 HUMAN RISKS IN INFORMATION SYSTEMS SECURITY

The behavior of people is quite different than that of computer systems. While computers do as they are instructed and their strengths and weaknesses are a science of design and operation, people react to their surroundings and make decisions based on variable conditions. Gonzalez and Sawicka [21] went so far as to refer to human interactions as “the Achilles heel of information security.”

As new collaboration tools and storage mechanisms give information access to a variety of individuals, organizations must understand the risks caused by human access and interaction. The “new information technologies create not only new common opportunities, but also common vulnerabilities” [22]. It is those same enabling technologies
which increase risk, as “the potential of networks is only limited by our imagination. Unfortunately, in the security field, it’s been the bad guys who’ve been first to recognize this potential. Mass mailers hijacked our address books and contact lists a decade ago, and social networks are already being exploited to distribute malware” [4]. Risk is posed by not just the “bad guys.”

Sasse, Brostoff and Weirich [17] studied several situational password rule violations victimizing common workplace interactions. The first situation, “ambushing,” takes advantage of a user under pressure to force them into changing their password to something easy to guess. Another, “conflicting goals,” takes advantage of a user keeping their passwords easily accessible after being reprimanded for missing a deadline due to a forgotten password. A third, “requested disclosure,” features a caller falsely stating that he works for the company’s IT support and outright asking the user to share their password for an application update. Each of these simple situations gives unauthorized access based on how a user perceives the security of their password and how strongly they are motivated to suspect nonstandard requests. Kraemer and Carayon [23] further described accidental or human error breaches as being “violations of a non-malicious nature, the deliberate actions that deviate from CIS processes that may or may not result in decreased CIS performance.” Kraemer and Carayon also discussed Smith and Carayon’s concept of work systems as “having five elements: the individual, task, tools and technologies, environment and the organization” [23]. Later, Kraemer, Carayon and Clem [2] divided vulnerability themes into “external influences, human error, management, organization of CIS, performance management, policy, resource management, technology, and training.”

6 CASE STUDIES

Chu, Zhu, Han, Liu, Xu and Zhou [10] studied file-sharing options using DropBox. One feature is sharing data with a “secret URL,” where anyone with the special random-generated URL “can access the data without further authentication or authorization.” Content in DropBox can also be set to “public,” whereby anyone with the URL (a normal path with filename) can access the material, or “private,” where the data owner defines which users are allowed access. The secret URL option though has no visibility to file versions, it is truly just a randomly generated redirector to an existing file or folder location. If the file or folder is changed or deleted, the URL stays active and when another file or folder is uploaded with the same name, the secret URL will continue to function. A Google search for part of DropBox’s “secret” URL standard short path of “site:db.tt” offers tens of thousands of files which can be accessed without any authentication. Further, anyone with access to one folder can see each other person with access to that folder and if the folder was shared with a secret URL, they can share that URL and access with anyone else. The “uncertain identities” risk [10] allows an unregistered user to take a sharing invitation link and register any email address with DropBox to access the shared content. Although DropBox offers several options to users to make their data available only to intended parties, it is also very easy to inadvertently share information with others. Standard discretionary access control requires each employee to set, manage and remove permissions for their data.

Several recent major breaches have been attributed to human decisions or errors. In 2011, email service provider Epsilon was breached by a “spear-phishing attack” in which a link to malicious software was sent to employees and their choice to click the link installed the software hackers used to access sensitive [24]. Employees at credit card processing company CardSystems Solutions stored unencrypted Mastercard credit card numbers leading to a 2005 breach of 40 million
credit card numbers [25]. HM Revenue and Customs, the tax authority of the United Kingdom, lost unencrypted computer discs in the mail in 2007 containing personal information about 25 million UK citizens, and in 2009 a similar mistake by employees at the United States Department of Veterans Affairs released personal information for 76 million American veterans from a shipped unencrypted disk [25]. The South Carolina Department of Revenue was attacked with a malware application which stole employee usernames and passwords to grant malicious access to government data and systems [26]. eBay was also recently victim to a spear phishing attack [26]. Attackers sent an email to employees with links to a malware installation that gave them access to eBay systems. [26]. Both incidents required employees to click links which installed malicious software on their organization’s computers.

7 ADAPTING INFORMATION SYSTEMS SECURITY PLANNING FOR THE HUMAN ELEMENT

While we understand that people account for significant risk in information security, organizations seem less sure of how to adapt to mitigate such risk. Murphy, Schlarman and Boren [27] recommend leveraging organizational support from “four pillars that support the information security framework: senior management commitment, security vision and strategy, information security management structure, and training and awareness.” Fischhoff identified factors that can be used to build an evaluation matrix for risks based on an “Items x Hazards matrix” translated into “technological risk” and “severity” [27]. While this gives us a matrix, appropriate remediation requires planning for the people interacting with such risks.

Training is a key shortcoming in information systems security planning. PWC’s “Information Security Breaches Survey Technical Report” [9] surveyed organizations for their “main driver for information security expenditure” and found more than half of responses to be “protecting customer information” and “preventing downtime and outages.” Despite their dedicating funds to these initiatives, only “26% of respondents with a security policy believe their staff have a very good understanding of it; 21% think the level of staff understanding is poor” [9]. They directly correlate ongoing security awareness training for employees with stronger understanding of security policy as a whole, with “36% of organisations that have an ongoing [security awareness] programme feel their staff have a very good understanding of policy, versus only 13% of those that train on induction only and 9% of those that do nothing” [9]. The impact of any security awareness training program is already evident. “Even the best firewall will not stop the best attack or recognize a new one. The only thing that helps are people who have been properly trained” [28]. But the number of organizations with ongoing staff education programs still lags behind the number of organizations suffering security breaches.

Culture is sometimes difficult to define and can be challenging to control, but is important in driving people to understand and behave in accordance with information security objectives. Johnson and Scholes defined organizational culture as those patterns of assumptions, or heuristics, that individuals will use as guidance when responding to a situation in the organization that they have not faced previously [18]. Three dimensions of organizational culture were defined by Aschenden [18], observable behavior of individuals; norms, attitudes and perceptions that can be inferred from what they say and do; and core values. Such core values are often discussed by organizational leadership but usually in terms of teamwork, integrity, community involvement and other highly visible or obvious ethics. Culture then is a combination of behaviors and attitudes in the workplace which play into the decision making of employees. But do executives discuss the
importance of diligence in handling sensitive information and the organization’s information systems security plan and expected behavior?

To further understand employee behavior and plan to encourage acting in accordance with best practices for secure information, we need to look at modern human behavioral theories. Functionalism suggests that culture serves the needs of an individual and the key role is “played by customs, rituals, and moral standards, which regulate the behavior of people” [22]. Astakhova [22] further defined information security culture as “a specific mode of the organization and development of a subject’s information activity, which is represented in the value-oriented models of his information interaction as a sender and receiver of information, under which he determines and controls the unity of existence and development of information objects in their cognitive and communicative manifestations.” The mention here of value orientation and subject control hold significant weight in the role of users in information security. The organization needs to offer value or at least perceived value to employees for following best practices for secure information. Its processes must encompass best practices for security without complicating tasks.

Other behavioral theories also help explain how employees may react in the workplace. The elaboration likelihood model (ELM) by Petty and Cacioppo [29] explains attitudinal change caused by personal circumstances upon receiving a persuasive message. ELM defines two processing routes for persuasive messages, either the central route by which a message is scrutinized, understood, and then behavior chosen, or the peripheral route when the receiver does not understand the message and is more affected by other indirect factors such as trust for the sender of the message [30]. Rogers’ protection motivation theory [30] suggests threat perception is constructed by several factors, “perceived severity,” “probability of occurrence,” and “cost” [30]. Negative factors influencing perception would include “response efficacy” and “self-efficacy” [30].

Another key component of human behavior is perception. “Perception is a major part of human intelligence and a key component to understand human behaviour… it is the mechanism with which a person evaluates external inputs, which, in turn, determines the behavioural response” [2]. People need to understand the technology they use in the workplace, its risks and all the security controls designed to use with it. “Whether people are willing to adopt an IT appliance depends not only on its ‘real security level’, but also on its ‘perceived security’” [2]. The psychometric paradigm suggests people perceive risk by considering familiarity of risk, severity of consequences, and knowledge about risk [31]. Employees are therefore surrounded by influencers and the organization and its leadership controls what information reaches the employee, helps craft perception and guides response. An organization’s influence on perception can then help control behavior.

To build an effective information security function, we need to take account of the skills available, the needs of the business, and the politics of the day. There is no single structure that will work best in all circumstances. And new structures rarely survive for long, because of frequent business restructuring. We also need to take account of the periodic ‘pendulum swing’ between centralization and devolution of political power. [4]

8 CONCLUSIONS

With information being key to business operations and success, and the security of that information reliant on employees, several components must work in harmony to form the organization’s information systems security plan. Scholars have identified the human component of information security as a key and
sweeping risk, yet few have proposed actionable solutions. They clearly emphasize the importance of understanding employee behavior and molding information systems security planning to nurture and direct that behavior. Yoon and Kim [32] found multiple influencers of employee behavioral intent, including security policy, organizational norm, moral obligation, subjective norm (social pressure), perceived threat severity, perceived threat vulnerability, response efficacy (effectiveness), self-efficacy and attitude. Huang, Rau and Salvendy [2] focused more on human perception of issues and information which influence user behavior. Gonzalez and Sawicka [33] recommended an “interdisciplinary approach” to improve information systems security, combining components from technology, information science, psychology and management. Astakhova [22] defined information security culture as “a specific mode of the organization and development of a subject’s information activity, which is represented in the value-oriented models of his information interaction as a sender and receiver of information, under which he determines and controls the unity of existence and development of information objects in their cognitive and communicative manifestations.” Thompson [15] expands on planning for the human element, encouraging “abstract and conceptual” education for users rather than specific “prescriptive and actionable” advice to encourage users to truly understand information security threats. Sasse, Brostoff and Weirich [17] proposed the Information Security Management Protocol (ISMP) to provide a framework for information security management planning including planning for human interaction. Each study recognized the importance of a more diverse information systems security program and the value of appealing to employees as people, rather than focusing on tools and technical security.

We know human behavior favors job efficiency rather than emphasizing secure practices. We understand the importance of managerial support and security culture. The security policy is the basis for telling employees how to safely interact with computer systems. The cliché interviewee comment, “I’m a people person,” suggests that an individual enjoys interacting with colleagues at the workplace and prefers human to human communication over working with machines. Why then do we show them on a screen or hand them in writing the company security policy and expect their thorough understanding, precise compliance and safe decision making?

9 RECOMMENDATIONS

Planning for human use and behavior is vital in information systems security. A balanced information systems security program in any organization, then, must involve careful planning for technology, policy, standards and norms, education, and culture. As shown in Figure 1, the core I.T. technology and policy can be outweighed by the effects of the organization’s standards and norms, education and culture. Each component has unique requirements and demands different actions from the business, such as technology requiring the largest financial investment and culture necessitating political savvy. Each category must also have an established governance process, be regularly reviewed by senior management for effectiveness, and be updated for continual improvement.
Technology: Provide sufficient funding to purchase, configure and test security hardware and software based on international standards, and all such purchases should be reviewed for effectiveness and return on investment.

Policy: Write policies in a people-friendly language avoiding jargon and acronyms. It should be readable, understandable, and brief.

Standards and Norms: Craft processes in a simple, security friendly manner. To avoid employees working around security, processes requiring additional effort to maintain security should be changed. Default configurations should be as secure as possible to allow workers to complete their jobs securely, without the need to create their own secure processes.

Education: Conduct training sessions focusing on information security concepts, including best practices, practical skills sessions such as how to create a secure but memorable password and updates on new and frequent threats.

Culture: Senior management must champion the security culture, bringing security concepts into normal business meetings and supporting security initiatives and training.

10 REFERENCES


