# Making Security Policies Memorable: the First Line of Defense

**Bradley K. Jensen, PhD**
Microsoft Corporation
7000 State Highway 161
Irving, TX
USA

**Janet L Bailey, PhD**
**Shawn Baar, Graduate Assistant**
University of Arkansas at Little Rock
2801 S. University Ave
Little Rock, AR
USA

## Abstract

*The increase in security threats comes at a time when the corporate workforce is becoming more mobile, employees' need to collaborate both internally and with business partners is increasing, and corporations are facing escalating federal and state legislative scrutiny. As vulnerabilities and breaches rise and costs due to lost customer data spiral out of control, it is not surprising security remains a top concern for CIO's. The first line of defense against this ever-encroaching enemy is a well-written, well-communicated, and well-enforced information security policy. However, policies are only effective if employees can remember the important information contained in them. Business professionals participated in a study which showed color can be used to assist in retention and recall of important policy information.*

**Key Words:** Information security, security policies, policy awareness, working memory, color study, recall

## 1. *Introduction*

Since 2003, information security and privacy has been listed in the top-ten list of CIO concerns (Luftman & Derksen, 2012). This finding is not surprising considering the sheer volume, nature, and associated costs of security breaches along with legal responsibilities and responsible parties involved in these breaches. Even though cyber security is a part of the plan of the United States for economic recovery and global technological progress, allocating increased funds to implement security plans is often a hard sell, especially since attaching a dollar figure to risk aversions is often difficult (Ponemon Institute, LLC., 2009). As more studies have been done examining the costs of a security breach, it is becoming clearer that information security must be approached with coherent processes that are continually updated and enforced, an often formidable task.

While security breaches have increased in severity and frequency over the past several years only 40 percent have the tools, funding, and personnel to prevent, quickly detect and contain data breaches (Ponemon Institute, LLC., 2013b). Fortunately, research has shown that awareness of an organization's policy has the largest direct impact on program effectiveness and that positive awareness can be more important to reinforcing security behaviors than enforcements (Knapp & Ferrante, 2012).

## 2. *Cost of Security Breaches*

In a 2012, the average annualized cost of cybercrime was found to be $8.9 million a year, with breaches ranging in cost between $1.4 million and $46 million (Ponemon Institute, LLC, 2013a). And the outlook is not getting better. These companies experienced an average of 102 *successful* attacks per week, or 1.8 attacks per company. This represents an increase of 42 percent from the previous year. In each case, the reporting company lost confidential customer data. The majority of the reported costs resulted from lost business and associated costs (customer churn rates, legal defense, and public relations costs).

Information theft (44%) and costs associated with disruption of business or lost productivity (30%) account for the majority of external costs, while recovery and detection (47%) is the largest internal cost (Ponemon Institute, LLC. 2013b). Estimates of the cost to U.S. businesses alone range from a 24 billion to 120 billion dollars and the global cost of cyber activity is estimated to range from 300 billion to one trillion dollars (Lewis & Baker, 2013).

## 3. Vulnerable Systems

Several trends raise concerns about the growing vulnerability of systems. Most reports focusing on cyber security agree that companies face several evolving types of threats to their security. Three of the largest include threats that come from the increased use of mobile devices, malware on legitimate websites, and various forms of phishing techniques. While seventy-three percent of IT security professionals list employee errors and omissions as a top three threat perceived as being of high or average threat (Deloitte, 2013), these are also some of the easiest ones to prevent with a clearly communicated security policy.

### 3.1 Mobile Platforms

The explosion in popularity of "smart" mobile devices leaves enterprise networks more vulnerable to compromise if communication to and from these devices is not secure. Gartner predicts that by 2017, half of employers will require employees to use personal smartphones for work-related purposes (van der Muelen & Rivera, 2013) yet 60 percent of organizations view mobile devices as “IT security’s weakest link” followed by laptops and social media (Cyberedge Group, 2014).

In 2012, malware across mobile platforms grew 614 percent to 276,259 up from an increase of 155 percent in 2011 (Juniper Networks, 2013). Trend Micro predicts that Android will remain the dominant OS in the market. They further predict that the volume of malicious and high-risk Android apps will reach three million by the end of 2014 (Genes, 2014). To put things in perspective, in 2012 at 350,000 detected malicious and high-risk Android app samples, Android had taken less than three years to reach the number of malicious apps that it took Windows fourteen years to achieve (Trend Micro, 2013). While Google has attempted to address these security issues, not all users can take advantage of the security features due to the heavy fragmentation of the open-source OS (Genes, 2014). Additionally, there is always the threat the loss or theft of the devices themselves or failing to properly degauss a device containing sensitive data (Ponemon Institute, LLC., 2013b).

### 3.2 Web Browsing

Of additional concern is the number of compromised Web sites. In 2012, eighty-five percent of web sites containing malicious code were compromised legitimate sites, and the number of malicious web links grew nearly 600 percent worldwide. Cybercriminals are now targeting legitimate websites within certain categories that organizations are unable to block access to without affecting productivity (Websense, 2013).

### 3.3 Phishing

Phishing comes in many forms and has been around a long time. As companies evolve and learn from previous vulnerabilities (either theirs or someone else's), cybercriminals are also evolving. In the last year, these criminals have learned to send targeted, legitimate looking emails, often imitating legitimate messages from legitimate sources. All it takes is one employee to click on an infected link for criminals to gain access. They are even learning to exploit a design flaw in traditional email security systems. These defense systems generally only check any embedded links as the email hits its email server. Cybercriminals have started sending the email before infecting the link. After the email server's defense system places it in the recipient's inbox, the criminal compromises the targeted site. That same survey also showed that 50 percent of respondents checked their emails from outside the corporate network, either on mobile devices or from a remote desktop (Websense, 2013).

### 3.4 Bottom Line

Because people are part of the problem, they need to be part of the solution as well. Managing risks from exposure to new technologies require training and and awareness (Deloitte, 2013). During the first half of 2012, security measures and raised awareness reduced effectiveness of traditional security scams. Cybercriminals responded with more sophisticated techniques (Websense, 2013). Employees need security policies that keep them current on possible forms of vulnerabilities, policies that are easily remembered.

## 4. Information Security Policies

Two areas that collectively aid in the formation of security policies are legislative regulations and IT governance documents. As of the end of 2013 46 states in the U.S plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands had passed laws requiring notification to affected customers, employees, students, and other individuals when a breach of personal data occurs. The only states who have yet to pass this type of legislation are Alabama, Kentucky, New Mexico, and South Dakota (National Conference of State Legislatures, 2013)

After being in the top three list of security initiatives for 2012, security-related regulatory compliance did not even make the top ten this year. It has been replaced by security strategy and roadmaps, indicating how smart businesses are recognizing how crucial information security is to their overall success (Deloitte, 2013). Security policies are critical to IT governance documents. “Not having a policy is like not having a business plan –you’re driving without a map. When developing a policy, the clearer it is, the better it will serve you” (Fratto, 2008). However, a clearly written policy is insufficient; policies only deter risky behavior if employees read and adhere to them (Taylor & Brice Jr, 2012).

The purpose of an information security policy is to provide direction and support in the complex world of information security. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which collectively form a specialized standardization body responsible for development of the foremost industry standard for information security, state, “An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties” (ISO/IEC, 2005). Security policies include not only basics like definitions of what constitutes security, overall objectives, scope, and the importance of protecting corporate data but also general statements of intent, definitions of general and specific responsibilities for security management, and references to supporting documentation. Perhaps most important in today’s marketplace, though, is for the security policy to include a brief explanation of the principles, standards, and compliance requirements for the organization, such as the following:

1. compliance with regulatory requirements.
2. security education.
3. malware prevention.
4. business continuity planning.
5. individual best practices.
6. consequences of security policy violations (ISO/IEC, 2005).

Figure 1 presents the “Plan Do Check Act” (PDCA) model developed by the ISO/IEC to structure all Information Security Management Systems (ISMS) processes. Evaluation of the PDCA illustrates that policies are at the heart of corporate information security.

To assist organizations, the IT Governance Institute provides *Control Objectives for Information and related Technology (COBIT)* (IT Governance Institute, 2007). The mission of this framework is to “research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals” (p. 9). According to COBIT, information must satisfy business objectives by conforming to the following quality, fiduciary, and security criteria:

1. Effectiveness.
2. Efficiency.
3. Confidentiality.
4. Integrity.
5. Availability.
6. Compliance.
7. Reliability.

A major component of the COBIT IT governance framework necessary to ensure the success of business objectives is the communication from management regarding the goals and direction of the organization. Figure 2 illustrates the importance of policies to this process.

Unfortunately, all too often policies are outdated, forgotten, or not well communicated.

Furthermore, having a policy in place with which managers and employees are unfamiliar can lead to a false sense of security that may ultimately be more dangerous than having no policy at all (Contos, 2006). Creation and enforcement of a security policy is not an easy task. Research shows the only challenge greater than enforcing security policies is managing the complexity of security itself (InformationWeek Research & Accenture, 2007).

An integral step in enforcing a policy is to ensure a solid awareness of policy components. SANS suggests the inclusion of the following questions in internal audits:

1. Do managers know the mission statement?
2. What is the level of employee awareness of specific security practices?
3. Do employees know the policies and procedures for developing and protecting information systems and components?
4. Can internal auditors name a dozen technical security protective or detective controls without looking them up? (Wright, 2008)

Each of these questions requires at a minimum a basic knowledge of the company's security policy, thus illustrating the importance of retention of important policy information.

As organizations face an increasing number of rules and regulations relating to security, noncompliance can result in significant liabilities. Simply having policies for addressing the rules and regulations does not assure compliance. Regulatory requirements are only somewhat effective in improving the organization's security stance thus compliance monitoring was seen as essential (Buith, 2007).

## 5. Color and Retention

What can be done to help individuals retain security policy information? Would the use of color help? To date limited research has addressed the use and benefit of color on retention of important information. Previous studies have been conducted on the effect of color on memory retention in the medical arena using student surrogates (Lamberski & Dwyer, 1983; Dwyer & Moore, 2001). A more recent study tested the effect of color on memory retention of random words also using student surrogates (Bunting & Cowan, 2005). Prior studies have shown color produces substantially more accurate recall than shape and a larger disruptive effect of attentional load across all stimulus conditions (Allen, Baddley, & Hitch, 2006; Allen, Hitch, Mate, & Baddeley, 2012). Building on the findings of previous color studies, the research reported in this article focused on an analysis of the effects of color on the retention of security policy information in a business environment using business subjects rather than student surrogates.

## 6. Methodology

The primary research question was whether or not color would have an effect on retention of key business information by business people. A pretest/posttest control group laboratory experiment was conducted to determine the answer to this question. Anchoring regarding previous knowledge of the information retention task, in this case knowledge of the aerospace industry, an area the participants were intended to be unfamiliar with, was applied.

Participants consisted of sales personnel, general management employees, distributors, value-added resellers, and customers from a Fortune 100 computer-related equipment sales and manufacturing corporation. The experiment was administered during regular training sessions to groups of 4 to 14 volunteers at the corporation's main training facility. The test suite was administered 12 times to a total of 111 subjects.

The task consisted of reading a standard hard-copy business document. Experimental groups were given an achromatic document with key information presented in red. Control groups were provided with a document containing identical information presented in a chromatic format. A subject's performance was evaluated by the amount of key information retained. Subjects were tested for color blindness/deficiency; this factor was controlled for. Table 1 reflects the summarization of the application of research framework constructs, variables, and surrogates.

Two hypotheses were evaluated:

H1 For all subjects, use of redundant color to highlight important passages of security text will result in significantly higher retention rates than a pure black and white mode of presentation.

H2 For non-color-impaired vision subjects, use of redundant color to highlight important passages of security text will result in significantly higher retention rates than a pure black and white mode of presentation.

The parts of the test were administered in the following order:

1. Pretest questions pertaining to security-based material presented in the Industry Marketing Sales Strategy and Background report from the Aerospace Industry.
2. Industry Marketing Sales Strategy and Background Report with critical security materials from the Aerospace Industry.
3. Security information retention test questions from the Industry Marketing Sales Strategy and Background report with critical security materials from the Aerospace Industry.
4. Background Questionnaire.
5. Color Blindness Evaluation.

For validation purposes, five industry executives were asked to provide feedback on the pretest, posttest, and reading material parts. The executives qualified as experts in the field of aerospace industry security based on years of experience in industry marketing and aerospace marketing in addition to having a working knowledge of security issues within the aerospace industry. Each of the executives had between 12 and 24 years in industry marketing, between 2 and 24 years in aerospace industry marketing, between 2 and 38 years of experience in the aerospace industry, and a working knowledge of security issues within the industry. Each of the experts evaluated the appropriateness of the reading content along with the makeup and nature of the test instrument questions.

In addition to content validity, parts two and four were validated using the test-retest reliability, split-half reliability, and Spearman-Brown correction formulas. To perform this validation, nine business subjects from the Fortune 100 company facilities volunteered to take each part of the experiment twice over a two-week period.

Three of the subjects were given achromatic versions of the pretest, achromatic reading parts, and achromatic posttests. Three of the subjects were given achromatic versions of the pretest, chromatic reading parts, and chromatic posttests. The remaining three subjects were given achromatic pretests, chromatic reading parts, and achromatic posttests.

The split halves correlation for the pretest ranged from 0.0 to 1.0. The split halves correlation for the posttest ranged from 0.77 to 1.00. The correlation factors for the subject’s sessions as were obtained using the Spearman-Brown Correction formula. These results indicate that evaluation of the internal consistency reliability of the pretest is 87 percent and the posttest is at least 92 percent (see Table 2).

Part one of the test instrument was comprised of ten security-based questions of the same multiple-choice format used in part three of the test instrument. The intent of part one was to provide the subjects with an understanding of the nature and expectations of parts two and three, to provide an anchor point for subjects with prior knowledge of critical security issues within the aerospace industry, and to determine if a subject's prior knowledge is so extensive their answers would not be reflective of the influence of the use of color in hard-copy output.

Subjects were given three minutes to complete part one. No subjects during the twelve test administrations were unable to complete the ten questions in the allotted time. Questions for the chromatic and achromatic test versions were identical and were achromatic in presentation format. All security-based questions were multiple choice with the last option in all cases being "e: Do Not Know." All subjects were instructed not to guess on any of the answers.

Part two of the security-based test instrument was designed to provide identical information in chromatic and achromatic formats. A redundant color-coding scheme, which used red as the color code, was employed to highlight critical security information in the test instrument. The same fields that had the red color code applied in the chromatic version of the test instrument were bolded in the achromatic version of the test instrument.

The industry marketing sales strategy and background report containing critical security information was taken from an existing sales kit designed for use by industry marketing, sales, and management personnel for the Fortune 100 company where the testing was conducted. Part two was ten pages in length and contained tables, charts, and text. Care was taken to avoid the use of security terms that would tend to confuse subjects not familiar with critical security aspects within the aerospace industry. All subjects were given 16 minutes to read the security strategy and background report. All subjects completed the reading of the report in the allotted time.

Part three was comprised of 20 questions in the same multiple-choice format as those used in part one. The ten questions from part one were interspersed among the questions in part three.

Part three was administered to all subjects directly following completion of part two. As with part one, this part was timed so each subject had an average of 20 seconds per question.

The total time for part three was set at six minutes. All security-based questions were achromatic with no coding applied. Also, option”e: Do Not Know” was retained from part two so that subjects were required to provide an answer; and, again, subjects were asked not to guess.

Each subject completed the background questionnaire following completion of part three. The goal was to help establish any previous experience with industry marketing, security within the aerospace industry, and the aerospace industry in general. Subjects were also queried as to whether they had previously taken a color blindness test and if they were aware of having any form of color deficiency. A color blindness test was then administered using sixteen color plates. Each plate corresponded to the color codes employed in the test instrument and was taken from recognized color blindness tests (Ishihara, Tests for Colour Blindness: 38 Plates Edition, 1993; Ishihara, Tests for Colour Blindness: Concise Edition, 1994).

The complete test instrument was administered to subjects in single group sessions of approximately one hour in length. Equal numbers of chromatic and achromatic versions of the tests were randomly distributed during each of the 12 test administration sessions.

## *7. Analysis and Findings*

ANOVA was used to test the difference between population means. The first set of ANOVAs employed the total test population of 111 subjects, comprised of 56 chromatic and 55 achromatic scores. The second set of ANOVAs was performed on the total test population minus those subjects who possessed any form of color deficiency.

In the case of the posttest data, a separate set of ANOVAs was performed that accounted for the anchoring. Anchoring differences were achieved by subtracting pretest results from posttest results on a by-subject basis.

The results indicate when scores for all participants are included the only significant difference between achromatic and chromatic testing appears when anchoring is applied. However, when color-impaired subjects are removed from the sample, a significant difference is found (see Table 3). This finding indicates the use of color is beneficial in the retention of critical security information. Therefore, printed security policy manuals, memos, and other documents would benefit from the use of color to highlight the most important pieces of information. Caution should be exercised to avoid the overuse of color, however, lest the retention value of the chromatic text become synonymous with that of the achromatic text.

The test in this study only used black and red text in bold and regular type. Therefore, the findings are limited to security-based policy materials that would be published in formats such as reports, emails, newsletters, memos, etc. Future research is needed to study the effects of colors other than red and black as well as the use of dichotomous color sets. Research should also be conducted to determine what percentage point of chromatic text constitutes “overuse” and thus negates the benefits.

## *8. Conclusions*

Eighty-five percent of security breaches are opportunistic attacks. Given the nature of these attacks, organizations would be wise to focus on ensuring essential controls are in place across the organization (Buith, 2007). A critical component of this process is the enforcement of corporate security policies that must be communicated to management and employees in a manner that facilitates the retention of information critical to the security of information systems.

The results of this study support the claim that greater retention of critical information occurs when color is used to highlight important text versus the application of redundant achromatic codes such as bolding. In a day and age where there are insufficient financial resources to provide the tools, personnel, and funding to quickly prevent security breaches, it is all the more important for organizations to provide policy documents, both printed and online, that highlight and support the memory of important information.

Future research will benefit from examining difference related to the use of multiple colors which could be used in posters, web page alerts, security reports, and multi-color newsletters. To fully utilize multiple colors, a study on the effect of colors on information recall other than red is also advisable.

As the volume and nature of connectivity continues to evolve with BYOD, cloud storage/computing, and social media, organizations will continue to face increasing risk. "Data breaches, cloud computing, location-based services and regulatory changes will force virtually all organizations to review, and at least half of all organizations to also revise, their current privacy policies before year-end 2012.

These issues will dominate the privacy officer's agenda for the next two years (Gartner Says Half of all Organizations Will Revise Their Privacy Policies, 2013)." At a time when information security threats are mounting and costs of breaches are spiraling, the need for better, more effective information recall mechanisms is escalating. The task is daunting, but it is hoped the findings of this study will be useful as an initial step in the battle to protect organizations from ever-increasing threats.

## *References*

Allen, R. J., Hitch, J. G., Mate, J., & Baddeley, A. D. (2012). Feature binding and attention in working memory: A resolution of previous contradictory findings. *The Quarterly Journal of Experimental Psychology, 65*(12), 2369-2383.

Allen, R., Baddley, A., & Hitch, G. (2006). Is the binding of visual features in working memory resource-demanding? *Journal of Experimental Psychology: General*, 298-313.

Buith, J. (2007). *Treading Water: The 2007 Technology, Media & Telecommunications Security Survey.* New York: Deloitte.

Bunting, M., & Cowan, N. (2005). Working memory and flexibility in awareness and attention. *Psychological Research*, 412-419.

Contos, B. (2006). *Enemy at the Water Cooler.* Rocklan: Syngress.

Cyberedge Group. (2014). *2014 Cyberthreat Defense Report: North America & Europe.* Annapolis, MD: Cyberedge Group.

Deloitte. (2013). *Blurring the lines: 2013 TMT Global Security Survey.* San Francisco: Deloitte, LLP.

Dwyer, F., & Moore, D. (2001). Effect of Color Coding on Visually Oriented Tests With Students of Different Cognitive Styles. *The Journal of Psychology*, 677-680.

*Gartner Says Half of all Organizations Will Revise Their Privacy Policies.* (2013, 10 30). Retrieved from www.gartner.com: http://www.gartner.com/newsroom/id/1761414

Genes, R. (2014). *Blurring Boundaries.* Irving, TX: Trend Micro.

InformationWeek Research & Accenture. (2007). *Information Security Survey 2007.* www.informationweek.com/research: CMP United Business Media.

Making Security Policies Memorable 18

Ishihara, S. (1993). *Tests for Colour Blindness: 38 Plates Edition.* Tokyo, Japan: Kanehara Suppan Co.

Ishihara, S. (1994). *Tests for Colour Blindness: Concise Edition.* Tokyo, Japan: Kanehara Suppan Co. Ltd.

ISO/IEC. (2005). *Information technology - Code of practice for information security management.* London: British Standards Institution.

IT Governance Institute. (2007). *CobiT 4.1.* Rolling Hills, IL: IT Governance Institute.

Juniper Networks. (2013). *Juniper Networks Third Annual Mobile Threats Report: March 2012 through March 2013.* Sunnyvale, CA: Juniper Networks.

Knapp, K. J., & Ferrante, C. J. (2012). Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management Policy and Practice, 13*(5), 66-80.

Lamberski, R., & Dwyer, F. (1983). The Instructional Effect of Coding (Color and Black and White) on Information Acquisition and Retrieval. *Educational Communication & Technology Journal*, 9-21.

Lewis, J., & Baker, S. (2013). *The economic impact of cybercime and cyber espionage.* Santa Clara, CA: McAfee & The Center for Strategic and International Studies.

Luftman, J., & Derksen, B. (2012). Key Issues for IT Executives 2012: Doing More with Less. *MIS Quarterly Executive, 11*(4), 207-218.

National Conference of State Legislatures. (2013, 12 30). *State Security Breach Notification Laws*. Retrieved from www.ncsl.org: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Ponemon Institute, LLC. (2013a). *2012 Cost of Cyber Crime Study: United States.* Menlo Park: Ponemon Institute, LLC.

Ponemon Institute, LLC. (2009). *2009 annual study: U.S. enterprise encryption trends.* Menlo Park: PGP Corporation and Contu, Inc.

Ponemon Institute, LLC. (2013b). *The Post Breach Boom.* Menlo Park: PGP Corporation and Contu, Inc.

Taylor, R. G., & Brice Jr, J. (2012). Fact or Fiction? A Study of Managerial Perceptions Applied to an Analysis of Organizational Security Risk. *Journal of Organizational Culture, 16*(1), 1-23.

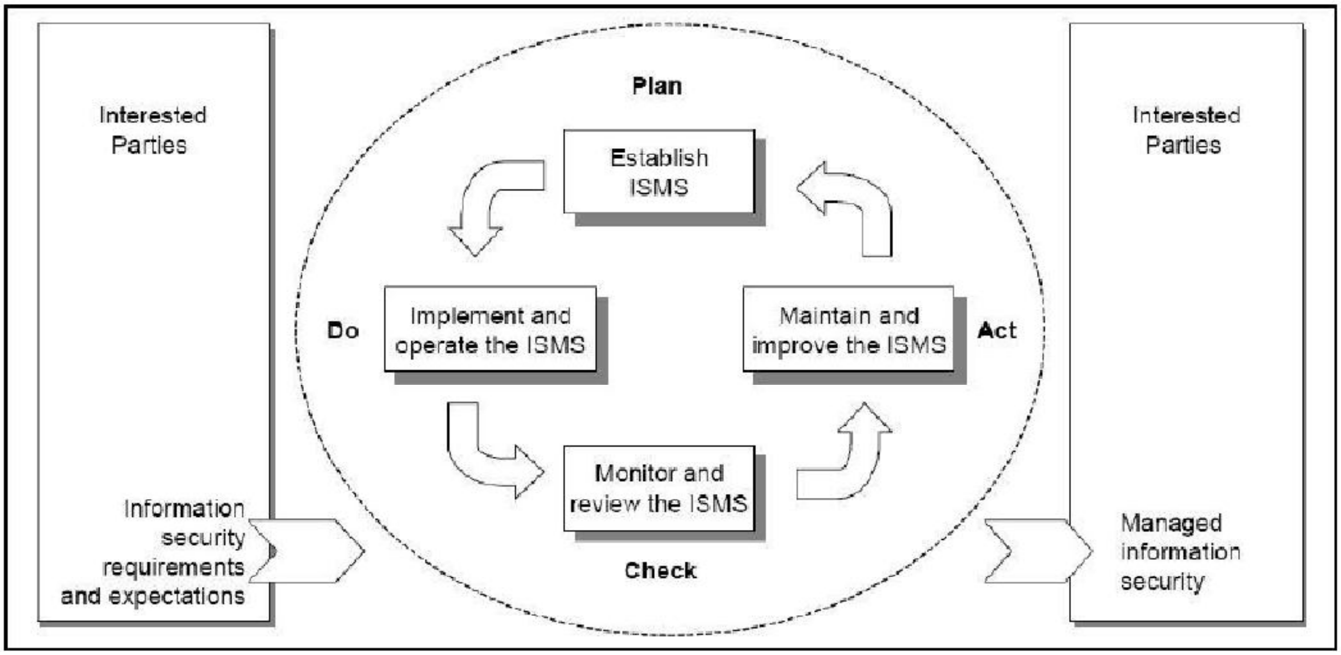
Trend Micro. (2013). *Repeating History: TrendLabs 2012 Mobile Threat and Security Roundup.* Irving, TX: Trend Micro.

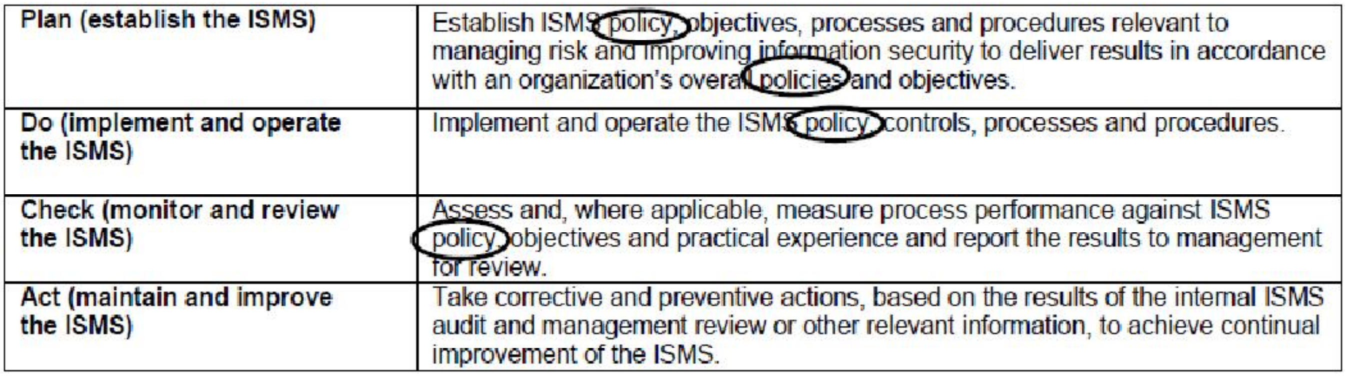
van der Muelen, R., & Rivera, J. (2013, 11 15). *Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes.* Retrieved from www.gartner.com: http://www.gartner.com/newsroom/id/2466615

Making Security Policies Memorable 19

Websense. (2013). *2013 Threat Report.* San Diego: Triton.

Wright, C. (2008). *The IT Regulatory and Standards Compliance Handbook: How to Survive an Information Systems Audit and Assessments.* Burlington: Syngress Publishing.

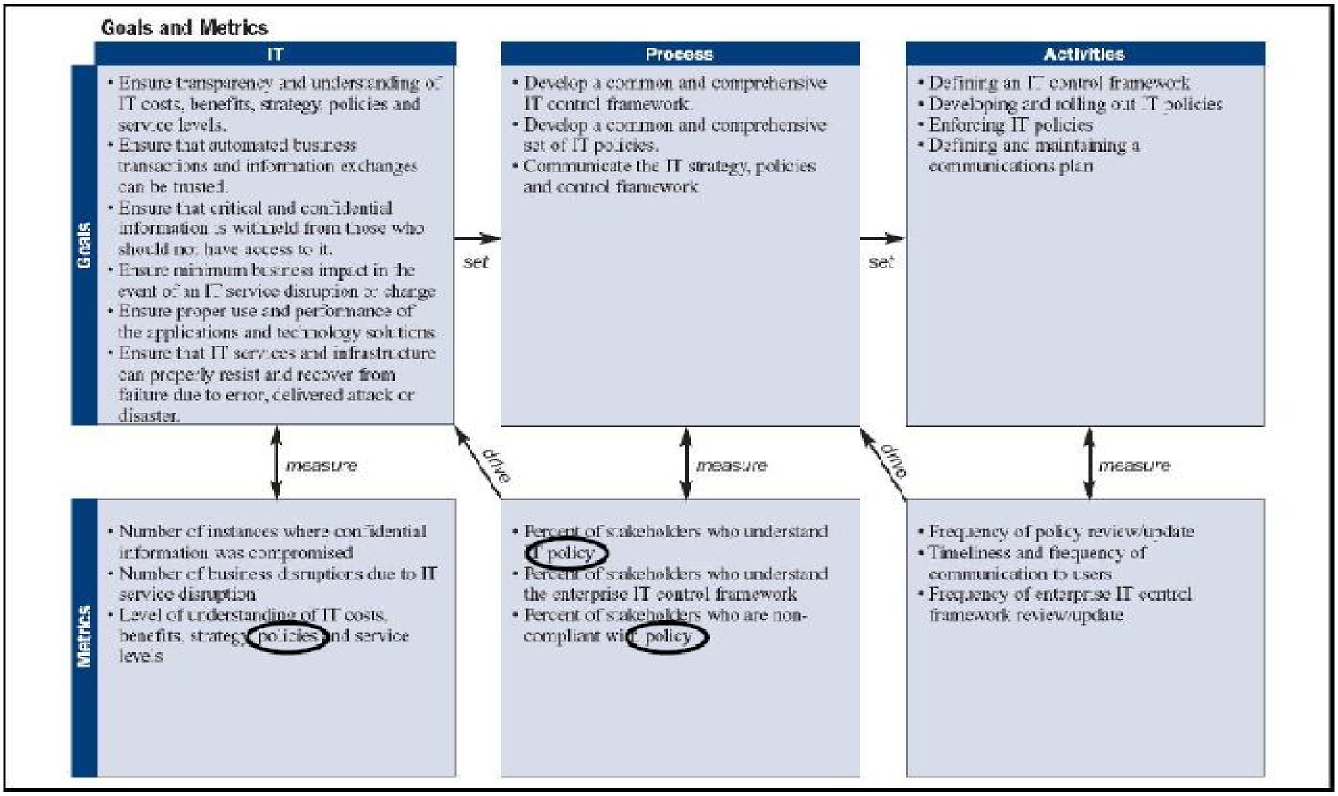

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security



| | |
|---|---|
| **Plan (establish the ISMS)** | Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives. |
| **Do (implement and operate the ISMS)** | Implement and operate the ISMS policy, controls, processes and procedures. |
| **Check (monitor and review the ISMS)** | Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review. |
| **Act (maintain and improve the ISMS)** | Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS. |

**Figure1. PDCA Model Applied to ISMS Processes**

**Source:** ISO/IEC 27001:2005(E) (2005).



IT – Goals:

- Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels.
- Ensure that automated business transactions and information exchanges can be trusted.
- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure minimum business impact in the event of an IT service disruption or change
- Ensure proper use and performance of the applications and technology solutions
- Ensure that IT services and infrastructure can properly resist and recover from failure due to error, delivered attack or disaster.

Process – Goals:

- Develop a common and comprehensive IT control framework.
- Develop a common and comprehensive set of IT policies.
- Communicate the IT strategy, policies and control framework

Activities – Goals:

- Defining an IT control framework
- Developing and rolling out IT policies
- Enforcing IT policies
- Defining and maintaining a communications plan

IT – Metrics:

- Number of instances where confidential information was compromised
- Number of business disruptions due to IT service disruption
- Level of understanding of IT costs, benefits, strategy, policies and service levels

Process – Metrics:

- Percent of stakeholders who understand IT policy
- Percent of stakeholders who understand the enterprise IT control framework
- Percent of stakeholders who are non-compliant with policy

Activities – Metrics:

- Frequency of policy review/update
- Timeliness and frequency of communication to users
- Frequency of enterprise IT control framework review/update

**Figure2. COBIT P06 Communicate Management Aims and Directions Goals and Metrics**

**Source:** COBIT 4.1 (2007).

**Table1 : Research Framework Constructs, Variables, and Surrogates**

| Construct | Variable | Variable Type | Surrogate(s) | Scale | Scale Characteristics |
|---|---|---|---|---|---|
| Physical Process | User Characteristics | Moderating | Color Blindness | Nominal | Ishihara Color Test |
| Mode of Presentation | Presentation Format | Independent | Color | Nominal | Chromatic / Achromatic |
| Task Type | Class of Problem | Control | Problem | Nominal | Structured / Unstructured |
| Performance | Outcome | Dependent | Information Retention | Ordinal | Number Correct |

**Table 2: Test Correlation Factors**

| | Test Administration | |
|---|---|---|
| Test Type | 1 | 2 |
| Pretest | 0.87 | 0.87 |
| Posttest | 0.92 | 0.95 |

**Table 3: ANOVA of Chromatic/Achromatic Results**

| Test Type | df | Mean Square | F-test | P-Value | F Critical |
|---|---|---|---|---|---|
| All Subjects | | | | | |
| Pretest | 1 | 0.497 | 0.155 | 0.694 | 3.928 |
| Posttest | 1 | 11.352 | 0.968 | 0.327 | 3.928 |
| Posttest w/anchoring | 1 | 65.441 | 5.670 | 0.019 | 3.928 |
| Non-color-impaired subjects | | | | | |
| Pretest | 1 | 0.006 | 0.002 | 0.965 | 3.943 |
| Posttest | 1 | 53.084 | 4.860 | 0.030 | 3.943 |
| Posttest w/anchoring | 1 | 54.261 | 4.758 | 0.032 | 3.943 |