Getting the Most out of Security Policies Through the use of Color

Bradley K. Jensen

Microsoft Corporation
214.674.3630
bjensen@microsoft.com

Janet L. Bailey

University of Arkansas at Little Rock
501.569.8851
jlbailey@ualr.edu

Amanda A. Jensen

Accenture, Inc.
214.707.5431
a.jensen3@verizon.net

Robert B. Mitchell

University of Arkansas at Little Rock
501.569.3383
rbmitchell@ualr.edu

ABSTRACT

The increase in security threats comes at a time when the corporate workforce is becoming more mobile, employees' needs to collaborate both internally and with business partners are 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 (Ponemon Institute, LLC, 2007) it is not surprising security remains a top concern for CIO's (McGee, 2008). The first line of defense against this ever-encroaching enemy is a well written, well communicated, and well enforced information security policy. This article reports the findings of a study that shows the use of color in the delivery of print and electronic training materials can assist in retention and recall of important information.

Keywords: Information security, security policies, color study, retention, recall.

INTRODUCTION

For the last three years, information security and privacy have consistently been ranked in the Top Ten list of CIO concerns (Luftman & Kempaiah, 2008; McGee, 2008). This is not surprising considering the sheer volume, nature, and associated costs of security breaches along with legal responsibilities and responsible parties for these breaches.

Vulnerable Systems

Several trends raise concerns about the growing vulnerability of systems. Foremost is the growing number of high-severity vulnerabilities which increased by 28 percent from 2006 to 2007. That trend continued into the first half of 2008, although at a much slower pace (Websense Security Labs, 2008). Web vulnerabilities which have tripled since 2005 to over 12,000 in 2008 now account for 51 percent of all vulnerability disclosures (IBM Global Technology Services, 2008). During 2007 alone, an average of 124 new vulnerability disclosures were made per day – a total of 6,437 for the year – of which nearly 90 percent could be exploited remotely (Aberdeen, 2008).

Of additional concern is the number of compromised sites. Seventy-five percent of all web sites containing malicious code are compromised legitimate sites – a number that has increased by almost 50 percent during the first half of 2008. During the same period, 60 of the top 100 web sites were either hosting or were affected by malicious activity.

Lost Data Expense

Another trend of concern to companies can be seen in the type of web attacks. Twenty-nine percent of malicious Web attacks were found to include data-stealing code and 46 percent of all data-stealing attacks have been documented as being conducted via the Web (Websense Security Labs, 2008). According to a benchmark study of actual costs conducted by Ponemon Institute, the total average cost of a data breach for each of their reporting companies was $6.3 million. The range of costs of these data breaches was between $225,000 and $35 million. Each of these reporting companies lost confidential customer data. The majority of the reported costs resulted

from lost business. In fact, costs associated with lost business now accounts for 65 percent of data breach costs. The study found contributing factors included increased customer churn rates, legal defense, and public relations costs (Ponemon Institute, LLC, 2007). Possibly more alarming is the fact that another survey found 36 percent of surveyed companies do not track losses of customer data while another 29 percent do not report losses unless required to do so by law (Buith, 2007).

Information Security Policies

Two areas that collectively aid in the formation of security policies are legislative regulations and IT governance documents. Sixty-eight percent of corporate security professionals report their companies must comply with one or more regulations; 20 percent – two; 13 percent – three or more.

Unfortunately, company policies have not kept up with the laws. As of 2007, at least 35 states in the U.S had passed laws requiring notification to affected customers, employees, students, and other individuals when a breach of personal data occurs (Ponemon Institute, LLC, 2007). Despite this, 49 percent of surveyed companies had not yet performed an inventory of customer data nor identified where all customer data resided within their systems (Buith, 2007). Most frighteningly, in a separate survey 56 percent of respondents reported their companies do not use an IT governance framework of any kind (Fratto, 2008).

"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 – it also needs to be clearly communicated and the information retained by employees and managers alike.

The purpose of an information security policy is to provide direction and support in the complex world of information security. "A policy document should be approved by management, published and *communicated*, as appropriate, to all employees" (ISO/IEC, 2000). Security policies not only include basics like definitions of what constitutes security, overall objectives, scope and the importance of protecting corporate data, they also include 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

1) Compliance with regulatory requirements;
2) Security education;
3) Malware prevention;
4) Business continuity planning;
5) Individual best practices; and
6) Consequences of security policy violations (ISO/IEC, 2000).

All too often policies are outdated, forgotten, or not well communicated. Unfortunately, having a policy in place that managers and employees are unfamiliar with 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 (see figure 1) (InformationWeek Research & Accenture, 2007).

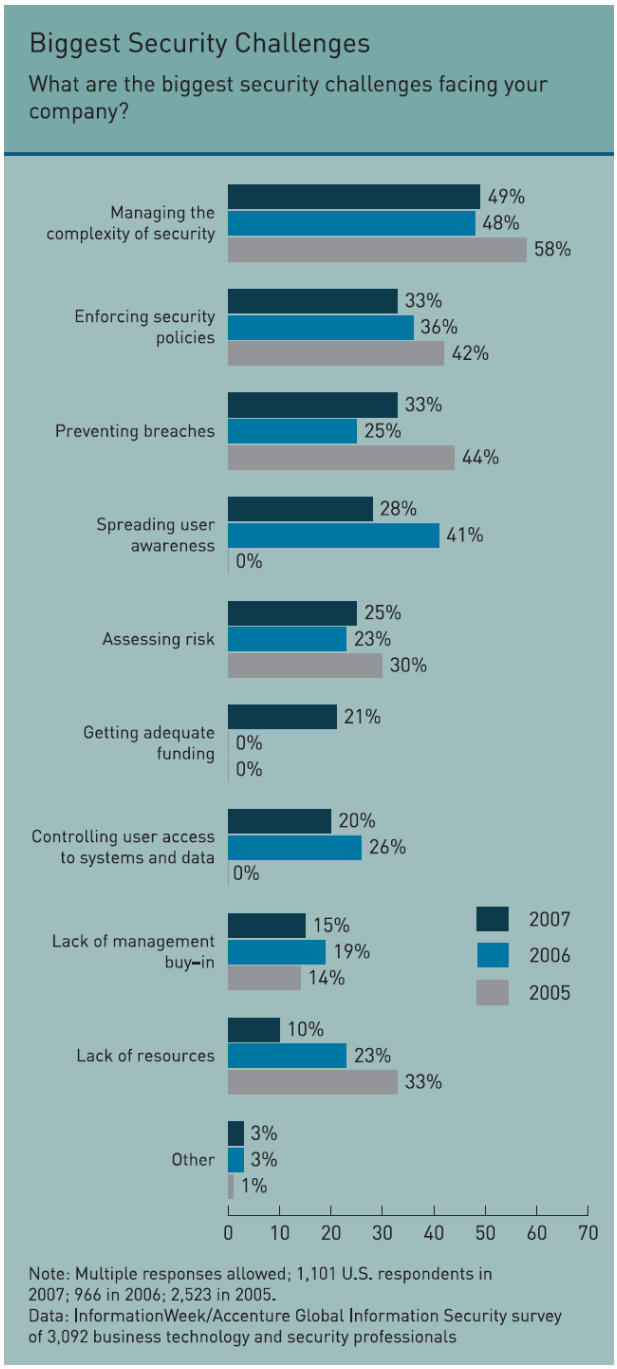

Figure 1: Security Challenges (InformationWeek Research & Accenture, 2007)

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 minimum a basic knowledge of the company's security policy thus illustrating the importance of retention of important policy information.

Color and Retention

The question is what can be done to help individuals retain this information? Would the use of color help? To date, there has been limited research to address 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). The design of the study reported in this article was to determine the effects of color in a business environment using business subjects rather than student surrogates.

METHODOLOGY

The primary research question was whether or not color would have an effect on retention of key business information by business people. To determine the answer to this question, a pretest/posttest control group laboratory experiment was conducted. 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 and this was controlled for. Table 1 reflects the summarization of the application of 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 1: 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.

In the order administered, the parts of the test were:

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 summarized in Table 3 were obtained by 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).

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

Table 2: Test Correlation Factors

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. There were no subjects during the twelve test administrations 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 sixteen 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, 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 twelve test administration sessions.

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 results 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. Such being the case, 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.

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

Table 3: ANOVA of Chromatic/Achromatic Results

It should be noted 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.

CONCLUSIONS

A benefit of the design of this research was the neutral redundant color code (i.e., bolding) used in the achromatic version of the test made the analysis more rigorous, thus making the positive performance findings even more striking. In general, the results of this study support the claim there is greater retention of critical security information when color is used to highlight important security text versus the application of redundant achromatic codes such as bolding.

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 task is daunting, but it is hoped the findings of this study will be used as an initial step in the battle to protect organizations from ever-increasing threats.

REFERENCES

Aberdeen . (2008). *Vulnerability Management.* www.aberdeen.com: Aberdeen Group.

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.

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.

Fratto, M. (2008). *2008 InformationWeek Strategic Security Survey Analytics Reporty.* Syracuse: United Business Media.

IBM Global Technology Services. (2008). *IBM Internet Security Systems X-Force 2008 Mid-Year Trend Statistics.* http://www-935.ibm.com/services/us/iss/xforce/midyearreport/xforce-midyear-report-2008.pdf: IBM.

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

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. (2000). *Information technology - Code of practice for information security management.* London: British Standards Institution.

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.

Luftman, J., & Kempaiah, R. (2008). Key Issues for IT Executives 2007. *MIS Quarterly Executive* , 99-112.

McGee, M. K. (2008, 9 3). *IT And Business Alignment Remains CIO's Top Concern*. Retrieved 9 4, 2008, from www.informationweek.com: http://www.informationweek.com/news/management/trends/showArticle.jhtml?articleID=210300331

Ponemon Institute, LLC. (2007). *2007 Annual Study: U.S. Cost of a Data Breach.* Menlo Park: PGP Corporation and Vontu, Inc.

Richardson, R. (2008). *2007 CSI Computer Crime and Security Survey.* GoCSI.com: CSI.

Websense Security Labs. (2008). *State of Internet Security.* http://www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf: Websense.

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