Strengthening Cybersecurity Series

A Best Practices Guide to Information Security

Clay Posey
University of Arkansas at Little Rock

Tom L. Roberts
Louisiana Tech University

James F. Courtney
Louisiana Tech University

IBM Center for
The Business of Government

TABLE OF CONTENTS

FOREWORD

On behalf of the IBM Center for the The Business of Government, we are pleased to present this report, *A Best Practices Guide to Information Security,* by Clay Posey, Tom L. Roberts, and James F. Courtney. This report comes at an opportune time for federal government leaders. In February 2011, the Government Accountability Office placed “Protecting the Federal Government’s Information Systems and the Nation’s Cyber Critical Infrastructures” on its High Risk List.

The report addresses how the human factor in information security has been the weak link in a much interconnected chain. Organizations take great pains to use technology to defend against outside attacks; they work hard to spot and stop the malicious insider who is willfully trying to do ill to systems. However, most organizations fall short in equipping their workers with best practices to make them part of the solution to information security.

The authors first describe the most common problems related to front-line information security, and then provide solutions to each of these problems. This report can be used to evaluate an established program, or to set up a new one. These solutions alone will clearly not stop every threat facing organizations in the information security arena, but they go a long way in closing gaps over which organizations actually have some control. Significant results can be achieved at little or no cost, and can reduce security “noise” so that security professionals can focus on the larger and more dangerous threats that remain.

While most efforts at training on information security focus on what not to do, the authors examine how to incentivize positive actions that organizations can take to improve collective security. This fresh perspective is one that everyone who comes into contact with government — employees, businesses, and citizens — can benefit from. We trust that this report will be useful to all government leaders as they work to prepare, train, and inspire their front-line workers to become stewards of information security.

Jonathan D. Breul

Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
jonathan.d.breul@us.ibm.com

Steven P. Bucci
Associate Partner
Cyber Security Lead, Global Leadership Initiative
IBM Public Sector, Global Business Services
spbucci@us.ibm.com

MOVING TOWARD A POSITIVE APPROACH

All organizations—public and private—currently face significant challenges in their ability to educate and motivate their employees about information security issues. Information security problems evolve at such a rapid pace that managers are challenged by the time demands necessary to truly understand key information issues —time normally allocated to daily operations. Despite increased attention to cybersecurity, limited funding for employee training presents a major challenge to organizations, especially government organizations. Much of the attention that is given to cybersecurity now focuses more on deterring detrimental actions by employees than on encouraging positive activities.

The overall goal of information security is straightforward—to protect an organization's information resources. Currently, organizations spend tremendous amounts of financial resources on acquiring new technologies whose manufacturers claim them to offer the greatest protective potential. Truth be told, however, the greatest resource that organizations have in protecting information assets is one they already possess—their own employees. This includes full- and part-time employees, temporary workers, and contracted individuals with authorized access to important organizational information. There is little doubt that these employees can pose significant security problems for organizations if they do not receive the education and training necessary to create a secure workplace which protects information and computerized information systems. With effort and a new approach which emphasizes positive security protection activities, organizations can help ensure that their employees will succeed rather than falter in the area of information security.

The objective of this report is to assist organizations in transforming employees into active partners in the protection of information resources. The authors believe that organizations should view their employees from this positive perspective. We believe that this perspective will assist employees in making information security more effective—much more so than the design and implementation of any new technology. To achieve this goal, organizations must concentrate on motivating and educating their employees to become and remain protective stewards of information.

The Questions and Answers presented in the report are derived from several years of research on information security and extensive interactions with both security professionals and thousands of employees at institutions throughout the United States. The Q and A section provides insights into what we have termed "protective security actions"—those activities that help protect information and the computerized information systems that create, store, or disseminate this information. The protective security actions described in this report should help form an internal, secure foundation for all organizations. This report provides a common-sense approach to better understanding an organization's internal information security environment and to assisting organizations in transforming employees to become a driving force for positive security efforts.

MOVING AWAY FROM A NEGATIVE APPROACH

It is a very difficult task for anyone to gain an in-depth understanding of a dynamic field like information security, especially when security is not their full-time, specified assignment. In addition, many employees' perceptions about information security are informed by media coverage of negative security events in both the public and private sectors. Examples of such negative events include:

- The ex-Transportation Security Administration worker who attempted to infect and corrupt a government database holding information about prospective terrorists[1]
- The largest U.S. military breach in history, caused by the insertion of a malware-containing USB flash drive in the Middle East in 2008[2]
- The hacking of the U.S. government travel reservation and reimbursement website, Govtrip.com, in early 2009[3]
- The 2009 loss of an external hard drive from the National Archives and Records Administration, containing personally identifiable information collected during the Clinton administration[4]

These events are certainly relevant to the security mission of government agencies. However, these examples only highlight the negative aspect of employee activities. As such, much if not all of the public discussion about security provides little or no insight into encouraging positive behaviors, as opposed to discouraging negative activities.

This report has been informed by the study of behavioral information security. This is the component of information security that examines the "human element" with both its positive and negative influences on organizational information resources.[5] Over the past several years, the authors sought the guidance of many information security professionals to obtain their views of what information security should be in organizational settings. More important, however, are the thousands of responses that we received from front-line employees in a myriad of industries. They informed us of their perspectives, understandings, and experiences related to information security. While security professionals' responses should be taken into consideration, it is the front-line employees who are in the trenches of daily organizational life and can provide first-hand accounts of their dealings with security-related issues.[6] This report is aimed at those on the front line working to improve the information security of their organizations.

LOGGING IN/LOGGING OUT

How can organizations work with their employees to improve security surrounding the logging-in process, including their use of ID and password? (p. 8)

How do you guard against employees using a computer workstation on which another co-worker has logged on? (p. 8)

What should organizations tell employees about setting a password? (p. 9)

What can organizations do to encourage employees to log out of the system as soon as possible after completion of their tasks? (p. 9)

WORKSPACE/WORKSTATION SECURITY

What can organizations do to get employees to lock their computer workstations before leaving their workspace? (p. 10)

What can organizations do to make certain that employees clear their desks of sensitive, physical documents at the end of the day? (p. 10)

Should organizations ever allow employees to install software on their workstations without receiving formal approval? (p. 11)

How quickly should employees apply updates to their workstations when notified to do so? (p. 11)

E-MAIL, SOFTWARE, AND INTERNET PROTECTION

How can employees evaluate certain risks in e-mails prior to opening them? (p. 12)

Prior to sending e-mail, should employees always double-check the list of potential recipients? (p. 12)

Should employees be allowed to send non-office-related e-mails (such as “chain” e-mails) to colleagues and friends while at the office? (p. 13)

Should employees use e-mail and Internet for personal reasons during office hours? (p. 13)

DOCUMENT PROTECTION

How long should employees keep sensitive documents before destroying them (if they ever destroy them)? (p. 14)

What is the best way for employees to destroy documents that they do not need anymore? (p. 14)

How often should employees back up important digital documents? (p. 15)

How much effort should employees expend in verifying the identity of communication recipients? (p. 15)

IDENTIFICATION AND REPORTING OF SECURITY MATTERS

How can organizations encourage employees to bring forth or even champion a new security idea? (p. 16)

What conditions of confidentiality are necessary to encourage employees to notify appropriate authorities about internal violations? (p. 16)

Should employees remind fellow co-workers of formally adopted security policies and standards? (p. 17)

ELECTRONIC DEVICE SECURITY

How can organizations communicate to front-line employees the security threats caused when USB drives, external hard drives, laptops, etc., are used without permission? (p. 18)

When out of the office (e.g., hotels, airports, elevators), how can employees attempt to limit their exposure to the threats around them? (p. 18)

LOGGING IN/LOGGING OUT

QUESTION: How can organizations work with their employees to improve security surrounding the logging-in process, including their use of ID and password?

ANSWER: Unfortunately, many employees admit to writing their ID and password down on post-it notes and attempting to hide them under a keyboard or a mouse pad. Many employees believe that:

- It is burdensome to remember a handful of IDs and passwords for each unique computer system.
- It is better for them to write this information down in order to remind themselves, rather than having to bother the IT personnel to relay this information back to them.

Employees should be aware that writing such information down is not acceptable. Organizations, however, must make an attempt to limit or consolidate the number of IDs and passwords in order to ease employees' cognitive effort in memorizing such login information.

Organizations should consider the use of biometric technology (e.g., face recognition, fingerprint, hand geometry, and voice analyses) to complement the traditional use of login criteria. While these technologies are not perfect and can be costly, they help decrease employees' cognitive load in remembering a handful of IDs and passwords, while increasing an organization's ability to identify users of their computer systems.

QUESTION: How do you guard against employees using a computer workstation on which another co-worker has logged on?

ANSWER: In some cases, employees will use a workstation in a shared environment (e.g., hospitals where many staff utilize the same programs on the same workstation to input or update patient information) even when a fellow co-worker is already logged into the system.

Organizations should consider the repercussions of such activities, as these actions limit the ability to attribute the changes in the system to the appropriate individual should an error occur. Employees must understand the potential issues of using a computer under someone else's logged session, as they can be held accountable for actions taken under their session.

Organizations must decide if this is currently happening, and, if it is, they must determine whether it should be considered an acceptable practice. Employers should hold employees accountable for logging off a computer workstation when they are not using it, especially if workstations are shared.

QUESTION: What should organizations tell employees about setting a password?

ANSWER: As a general rule, passwords should consist of a combination of lower- and upper-case letters, numbers, and special characters (e.g., %, @, &, #, !). These passwords should not include words in the English dictionary due to hackers' brute-force dictionary attacks.

In addition, longer passwords are usually more secure than shorter ones. Organizations typically require employees to change their passwords once every quarter. Organizations should be well aware, however, that employees are prone to using a series of a few different passwords in a round-robin fashion in order to satisfy this policy.

QUESTION: What can organizations do to encourage employees to log out of the system as soon as possible after completion of their tasks?

ANSWER: It should never be considered acceptable for employees to leave themselves logged into systems after they are finished using the workstation. Individuals who fail to log out in a timely fashion are leaving a window of opportunity for someone else to gain access to a system under their authorized access. Should such unauthorized access occur and important information be altered or destroyed, attribution cannot be made accurately, thereby holding the logged-in employee accountable rather than the real perpetrator.

Employees should quickly log out of the organization's IT systems upon completion of their tasks within those systems, or the systems should be set up to automatically logout employees after a certain amount of time of inactivity (on the system).

WORKSPACE/WORKSTATION SECURITY

QUESTION: What can organizations do to get employees to lock their computer workstations before leaving their workspace?

ANSWER: One very simple way that employees can protect sensitive digital information is to set their screen savers to password protect or to log out of their workstations prior to leaving the office space. This setting forces the user to enter a password when attempting to regain access to the workstation once the screen saver has been initialized.

As simple as this procedure may be, organizations need to be aware of how employees may feel about these procedures. Many employees attempt to justify not locking their workstation if they believe that they will only be away from their desk for a few minutes.

Research shows that individuals who believe that they will be gone for less than 10 minutes will purposefully not lock their systems, because they perceive that is not enough time for potential security threats to occur. Organizations should let their employees know that workstations should always be locked when they leave the workspace, regardless of estimated time of absence from the workstation. And should they forget, the automatic logout feature should assist in limiting unauthorized access by individuals.

QUESTION: What can organizations do to make certain that employees clear their desks of sensitive physical documents at the end of the day?

ANSWER: Just like an open computer system, sensitive physical documents left out in the open are subject to human security threats—even from the night janitorial staff. Employees should ensure that important documentation is stored in a locked drawer or file cabinet at the end of the workday.

Additionally, employees should also clear sensitive documentation from their desks between meetings in their offices. Individuals who visit an office may have a tendency to let their eyes roam along the surface of a desk, and leaving sensitive information there exposes it to visitors who may not have authorized access to such information.

QUESTION: Should organizations ever allow employees to install software on their workstations without receiving formal approval?

ANSWER: Some employees may consider it a burden to their IT department to request installation of software which the employee believes is necessary to doing their job effectively. Organizations should make it known to employees that software applications need to be evaluated by appropriate authorities within the organization prior to their downloading and installation on internal computer workstations and systems. Employers need to communicate that it is far better to "bother" the IT department with such requests than to recover from the aftermath of an executable file carrying malicious components.

In addition, organizations must comply with software licenses. Unfortunately, employees often load unlicensed software on the office workstations, which can lead to heavy fines for organizations. Software audits are key to minimizing these problems. Government organizations, like other entities, are not immune to licensing problems, so they must make sure that all employees are aware of their external-software policy. Furthermore, government organizations must comply with FISMA 2002 mandates which are required to inventory information systems within the agencies and show evidence of compliance with software licenses.

QUESTION: How quickly should employees apply updates to their workstations when notified to do so?

ANSWER: Many individuals are guilty of postponing the updates to personal computers at home simply because they do not want to be bothered with the hassle of a computer reboot. Unfortunately, this same behavior can be seen in the workplace.

Organizations should communicate to employees that updates should be applied as soon as possible on agency workstations and that they must not wait before applying the requisite changes. It should also be emphasized that employees should only apply updates if the appropriate personnel within the agency have made such a declaration, because hackers are now utilizing software update notifications as a way to infiltrate private organizational systems.

E-MAIL, SOFTWARE, AND INTERNET PROTECTION

QUESTION: How can employees evaluate certain risks in e-mails prior to opening them?

ANSWER: Employees generally have difficulty in assessing what determines whether an e-mail is considered a legitimate business request. Despite this, many employees admit that they open e-mails whose content is believed to be a bit suspicious (e.g., they do not know the sender, were not expecting the communication attempt, or the message did not seem to fit directly with ordinary work tasks).

Employees must be made aware of the threats posed to their organizations when handling e-mails, and just how quickly those threats can spread from one computer node to another inside a private network. Employees should never open e-mails—or worse, open the attachments within these e-mails—should the individual question the e-mail's purpose or sender. Employees should contact the authorized security personnel within their organizations to help verify the validity of electronic communications under conditions of uncertainty.

QUESTION: Prior to sending e-mail, should employees always double-check the list of potential recipients?

ANSWER: Yes. Employees tend to become hurried when sending information electronically and sometimes send sensitive information to the wrong recipients. Employees should be encouraged to pace themselves and to double-check both the content of the e-mail and the recipients of the e-mail to ensure that only individuals who are authorized to view such information actually receive the electronic communication.

Specifically, employees should review the "To:," "CC:," and "BCC:" entries prior to hitting the send button. In a recent example of employees who act too quickly, one of the authors received two follow-up e-mails—one from a major retail chain and the other from a major restaurant chain—on the same day in November 2010 that apologized for sending out the wrong information to customers just hours before. While these organizations worked to correct their issues in a post-hoc fashion, it is imperative that employees understand that e-mails cannot be recalled no matter how desperate their plea.

QUESTION: Should employees be allowed to send non-office-related e-mails (such as "chain" e-mails) to colleagues and friends while at the office?

ANSWER: All e-mail not specifically related to the daily functions of an organization should be strongly discouraged. While a bit of humor may often break the monotony of daily work tasks, an abundance of such material flowing within an organization's private network infrastructure can be quite disruptive and may have a potential of carrying malicious code with it. For these reasons, employees should be instructed not to forward such content to their colleagues, as they may unknowingly assist hackers in their attempts to break into the agency network.

QUESTION: Should employees use e-mail and Internet for personal reasons during office hours?

ANSWER: One of the most significant challenges now facing organizations is how to deal with the seemingly harmless utilization of Internet and e-mail by employees for personal purposes while on the job. Employees often think that if their work is completed within a given time frame, they should have the ability to browse websites such as eBay, check their personal banking accounts, or update themselves on the latest sports scores (the NCAA basketball tournament termed March Madness is one of the more subscribed sporting events within U.S. organizations).

It has become clear that the more time employees spend on the public Internet infrastructure, the more susceptible they are to information security threats. Such activities also place great stress on the organization's network infrastructure. If an organization chooses to block employees' personal use of e-mail or the Internet, the organization must clearly explain why this standard was set.

DOCUMENT PROTECTION

QUESTION: How long should employees keep sensitive documents before destroying them (if they ever destroy them)?

ANSWER: Both public and private organizations are paying increased attention to the sanitization of sensitive documents and electronic mail. A large part of this concern is the use of these documents in legal proceedings. In the wake of the Microsoft antitrust lawsuit, the Enron case, and the loss of White House e-mails during the Bush administration, the current legal guideline is to keep documents for a "reasonable time."

Organizations are responsible for interpreting the definition of "reasonable time." Currently, organizations in both the private and public sector are adopting policies on document sanitization that range from 30 days to five years. Organizations should establish sanitization policies and communicate those policies to employees.

QUESTION: What is the best way for employees to destroy documents that they do not need anymore?

ANSWER: When it comes to paper-based documents and reports, employees may simply forget to shred these physical copies, instead throwing them into the garbage bin with little or no effort provided to mask the information contained within. While employees may be aware that outside individuals engage in dumpster diving to acquire important organizational information, they must also be made aware that even the night janitorial staff can pose a security threat to information resources.

With digital information, the destruction is much more complex. Modern forensic software allows the recovery of many files that were previously deleted, or of information on digital media that has been overwritten or formatted. For this reason, the organization should adopt a digital shredding technique and media sanitization policy for hard drives and flash drives.

QUESTION: How often should employees back up important digital documents?

ANSWER: Organizations need to ensure that all employees are aware of the importance of the documents that they deal with directly. The challenge is the sheer number of documents, which in some organizations can actually reach into the millions.

A related challenge is the need-to-know policy that especially impacts many government entities dealing with classified information. Sometimes government managers don't have access to much of the information. The bottom line is that agencies need to set a policy for completing backups to ensure that agency operations continue in case of a disaster or system failure.

The timing of backups will vary, depending on the criticality of the documents being used by the agency. This timing can range from a matter of minutes to once a week. If this process is not already automated, organizations should begin with backup operations at least once a week—perhaps at the end of the workweek on Friday. The key, however, is to make sure that everyone knows the organization's backup policy and is consistent.

QUESTION: How much effort should employees expend in verifying the identity of communication recipients?

ANSWER: Much anecdotal evidence supports the idea that security threats are successful because employees fail to effectively determine the identity of their conversant. Threats known as social engineering attacks[7] are of formidable concern for all organizations, as they specifically target the emotions of employees to lead them into releasing important information to unauthorized individuals. Employees must make every attempt to verify the identity of every individual to whom they are releasing sensitive information.

In addition, social engineering attacks may be passive in nature. The attacker gains information about the employee to simply "crack their password" and gain access to the organization's systems. This could be as simple as asking about the employee's dog's name or college's mascot. Organizations must have clear-cut directions or checklists available to all employees to aid in this process and to make them less susceptible to social engineering tactics. For example, what questions could be asked of an individual to determine how to make it more difficult for a hacker to breach security? Just knowing the last four digits of a social security number is no longer a substantial hurdle for individuals who pose as others. Organizations should use the information—perhaps the non-traditional information—that they currently have about an individual to devise the components of such checklists. Additionally, employees must be made aware that such non-traditional information may be useful to hackers.

IDENTIFICATION AND REPORTING OF SECURITY MATTERS

QUESTION: How can organizations encourage employees to bring forth or even champion a new security idea?

ANSWER: In their daily activities inside and outside the workplace, employees may discover valuable security information pertinent to their organization. Unfortunately, many employees:

- Assume that the "IT security people" already know this information
- Are not comfortable in approaching individuals of a higher security status within the agency, for fear of being looked down upon or ridiculed

Organizations should work toward a culture in which employees are encouraged to bring forth new information and to share that information with their fellow co-workers and supervisors. Security managers should not discount the information received from "ordinary" employees simply because they do not have a formal education or specialization in information security matters.

QUESTION: What conditions of confidentiality are necessary to encourage employees to notify appropriate authorities about internal violations?

ANSWER: One of the major ways that organizations can use front-line employees as protective stewards is to encourage them to quickly notify proper authorities when they believe something or someone in their environment is, or has been affected by, an information security threat.

Concern about being labeled a "tattletale" or a "whistleblower" is common among employees. This is especially true of potential information security breaches. Organizations need employees who are willing to step up and inform the appropriate personnel when something out of the ordinary happens, without fear of retribution.

Organizations should find ways to encourage individuals to speak up about other employees who are not following formally accepted rules and who present a danger to information resources. An essential step in encouraging such behavior is to guarantee confidentiality and discretion in such matters. If an employee has even a limited degree of uncertainty regarding whether his or her name will be associated with the information provided, that degree of uncertainty may force him or her to withhold pertinent information.

QUESTION: Should employees remind fellow co-workers of formally adopted security policies and standards?

ANSWER: Employees are a very important resource for one another—perhaps more than the organization realizes. Often, an employee who is presented with a potential security threat will entertain suggestions from fellow co-workers about how to handle the issue. Organizations should use this to their advantage by actively searching for information security champions within their organizational units. These employees can act as liaisons between the IT security personnel and the individual units.

ELECTRONIC DEVICE SECURITY

QUESTION: How can organizations communicate to front-line employees the security threats caused when USB drives, external hard drives, laptops, etc., are used without permission?

ANSWER: Front-line employees must understand that electronic devices can pose severe security threats to the private, internal environment of the agency. Personal electronic computer equipment can wreak havoc for network administrators who attempt to protect the internal telecommunications networks. Not only do organizations have to be concerned with the potential for an individual to download and steal massive amounts of sensitive data in a short period of time with the aid of these devices, but the devices can also carry malicious code that only executes when the device is connected to a secure network. It is in an organization's best interests to limit or altogether ban the entrance and utilization of these technologies within the workplace.

QUESTION: When out of the office (e.g., hotels, airports, elevators), how can employees attempt to limit their exposure to the threats around them?

ANSWER: Employees must understand that security threats exist in many locations—the individual sitting next to them at the airport or on an airplane, standing in the elevator with them, or attempting to eavesdrop on a phone conversation conducted while eating a meal or drinking coffee. Accordingly, employees should attempt to distance themselves from other people when outside the traditional workplace. They should consider using privacy filters for laptops to protect confidential information, and should limit important phone conversations to areas where few or no other individuals are present.

It should also be communicated to employees that one of the least secure places for individuals working away from their organization is the wireless network of a hotel. Wireless networks have limited security to begin with, and may be easily compromised with hacking via packet sniffing or "Man in the Middle" techniques. This problem is made even more pervasive with the advent of smart cell phones. The process of tethering allows the phones to act as wireless access points for users around them.

If employees must utilize Internet services while on business, traditional, wired communications from known organizations are usually best. If employees must use wireless telecommunications links, they should evaluate the origin of the links and not just connect to the one with the strongest signal, which could be an individual attempting to filter the data packets' content as it is sent through the air.

Recommendation: Organizations must provide properly designed Security Education, Training, and Awareness (SETA) programs for all employees.

Both private and public organizations spend billions of U.S. dollars annually on Security Education, Training, and Awareness (SETA) programs for their employees.[8] While organizations believe that information security is an important topic on which to train employees, many do not understand how to do so appropriately. Consequently, the training employees receive from one organization can vary significantly from the training received in another organization. Our research shows that there is no standardization on:

- The frequency of SETA programming
- The approaches used to distribute this information
- The actual information provided in these sessions

For example, while some organizations supply security information daily to their employees via e-mail, others offer biannual, face-to-face group meetings in which they provide employees with pertinent information. Based on our research, 46 percent of employees have never received formal SETA efforts from their organization.

What, then, is the proper way to design and deliver SETA programs? Is providing some information necessarily better than providing none? Should this information be tailored to the organization whose employees are being trained? Regardless of the organization or industry, agencies can be more effective in their efforts by rethinking SETA. Think of SETA efforts as being composed of three, interrelated parts—the *what,* the *how,* and the *why*.[9]

- **The *what* is the awareness portion of SETA programs.** This component should be designed to inform employees of the security dangers lurking both inside and outside the organization.
- **Training covers the *how* of information security.** Training communicates to front-line employees the most appropriate ways to deal with security threats. This component must explicitly convey two key messages to the employees:
    - Employees must believe that the suggested responses to threats are actually effective. Without this perception, employees see no reason to engage in the suggested response other than “because the boss told me so.”

  - Employees must believe in their ability to carry out the suggested response effectively. Knowing about a suggested response is clearly not enough if an employee feels incapable of performing it adequately. Accordingly, organizations must not only educate employees but also provide them an opportunity to understand what they should do in the midst of security threats, and what specifically they should do to be successful.

- **Education covers the *why* of information security efforts within organizations.** This facet is perhaps the most important, yet most overlooked segment of SETA efforts. Individuals who understand the reasons why the organization is headed in a particular direction, or why individuals are interested in doing harm to the agency's information and information systems, are much better prepared in the fight against security threats. SETA programs must encourage employees to expand their view on security issues by exploring the consequences and actions to events that could happen, but are not normally experienced within a particular employee's office role.

ENDNOTES

1. Ex-TSA employee Douglas Duchak was charged in 2010 for his alleged actions of tampering with a database which housed data about potential terrorists targeting the United States. The malicious code could have had a much greater impact on the security of sensitive information had the government not stopped the execution of the code as early as it did.
2. In 2008, a USB drive containing malware was entered into sensitive military computer systems in the Middle East, causing the largest data breach that the U.S. military has ever encountered. This malware entered the system at a single point and spread quickly to other computer nodes—both classified and unclassified—throughout the military's network, thereby providing a formidable foundation.
3. Govtrip.com—a website used by government agencies for the travel arrangements and reimbursement of their employees—was hacked in 2009. This breach caused legitimate users of the website to be routed to an alternate web server where malicious code was downloaded to the users' machines.
4. In 2009, a hard drive containing records of more than 70 million military personnel was exposed to unauthorized organizations. This breach occurred simply because a malfunctioning piece of computer hardware was not properly erased prior to being returned for repairs.
5. Behavioral information security is a burgeoning discipline that covers all facets of how individuals can influence the protection of organizational information assets—both negative and positive influences. This discipline explores the interpersonal, organizational, societal, and cultural factors that affect individuals to harm or help protect these information resources (see Fagnot, I.J. (2008). Behavioral Information Security in L. J. Janczewski and A. M. Colarik (Eds.), *Encyclopedia of Cyber Warfare and Cyber Terrorism* (pp. 199-205). Hershey, PA: Information Science Reference.
6. It is important to incorporate the opinions and experiences of "traditional" employees along with those of information security professionals in order to develop better policies and procedures within firms. Studies that focus solely on information acquired from security professionals are inhibited as these professionals simply do not experience the day-to-day activities and interactions that employees at the operational level engage in (see Stanton & Stam, 2006).
7. Social engineering attacks rely on the interaction between an attacker and an employee—interaction that often takes advantage of an employee's willingness to assist a seemingly harmless individual—to gain access to important agency information assets. By far, the most (in)famous expert on social engineering attacks is Kevin Mitnick, owner of Mitnick Security Consulting, LLC. For more information about social engineering and information about successful attacks, see Mitnick's books entitled *The Art of Deception* and *The Art of Intrusion*. (see also Mitnick, K. (2003), or his article, "Are You the Weak Link?" *Harvard Business Review,* 81(4), 18-20.)
8. Of an annual IT security budget of $5.6 billion, the U.S. government allocates $140 to $150 million on security education, training, and awareness programs. Assuming that the U.S. government employs around five million individuals (including military and Postal Service), only $30 is spent per employee for SETA purposes (see http://www.informationweek.com/news/security/showArticle.jhtml?articleID=197008122).
9. Further information about SETA efforts can be found in the following texts: Whitman, M. E., and Mattord, H. J. (2007). *Principles of Information Security,* 2nd ed. Course Technology; Roper, C. A., Fischer, L. F., and Grau, J. A. (2005). *Security Education, Awareness, and Training: From Theory to Practice*. Butterworth-Heinemann.

ABOUT THE AUTHORS

Clay Posey is an Assistant Professor of Management Information Systems in the College of Business at the University of Arkansas at Little Rock. He received his D.B.A. from Louisiana Tech University in 2010 where his doctoral dissertation received full financial support from the United States Department of Defense Personnel Security Research Center (PERSEREC) in Monterey, CA. His research in information security has been published in several academic journals and presented at various national and international conferences. He is a member of the IFIP Working Group 8.11 / 11.13 on Information Systems Security Research.

Tom L. Roberts is the Clifford R. King Endowed Professor of Computer Information Systems in the College of Business and the Director of the Center for Information Assurance at Louisiana Tech University. He received his Ph.D. in Management Information Systems from Auburn University in 1993 and has previously held faculty positions at Middle Tennessee State University, the University of Central Florida, and the University of Kansas. He has published over 20 refereed articles and is also a member of IFIP Working Group 8.11 / 11.13 on Information Systems Security Research.

James F. Courtney is the Humana Foundation/McCallister Eminent Scholar Chair in Computer Information Systems in the College of Business at Louisiana Tech University. He received his Ph.D. in Management Science from the University of Texas at Austin in 1974 and has held faculty positions at Georgia Institute of Technology, Texas Tech University, and the University of Central Florida. He was also the Tenneco Professor of Business Administration at Texas A&M University. An expert in knowledge management and decision support systems, he has published nearly 50 articles in refereed journals.

ACKNOWLEDGMENTS

Many thanks go to Lynn Fischer, Kent Crawford, and all of the other individuals at the U.S. Department of Defense Personnel Security Research Center (PERSEREC) in Monterey, California, for their support and encouragement of our work in behavioral information security.

We would also like to thank the individuals at the IBM Center for the Business of Government for giving us the opportunity to help educate individuals within the government about behavioral information security. We hope that this report helps transform perceptions about employees' role in information security in the public sector.

To contact the authors:

Clay Posey
Assistant Professor of MIS
College of Business
University of Arkansas at Little Rock
2801 South University Avenue
Little Rock, AR 72204
(501) 683-7139

e-mail: mcposey@ualr.edu

Tom L. Roberts
Clifford R. King Professor of Information Systems
Director, Center for Information Assurance
Management and Information Systems Department
College of Business
Louisiana Tech University
P.O. Box 10318
Ruston, LA 71272
(318) 257-3514

e-mail: troberts@latech.edu

James F. Courtney
McCallister/Humana Eminent Scholar Chair in
Information Systems
Management and Information Systems Department
College of Business
Louisiana Tech University
P.O. Box 10318
Ruston, LA 71272
(318) 257-3804

e-mail: courtney@latech.edu

REPORTS from
The IBM Center for The Business of Government

For a full listing of IBM Center publications,
visit the Center's website at *www.businessofgovernment.org*.

Recent reports available on the website include:

Collaborating Across Boundaries

Environmental Collaboration: Lessons Learned About Cross-Boundary Collaborations by Kathryn Bryk Friedman and Kathryn A. Foster

Managing Innovation Prizes in Government by Luciano Kay

The Promise of Collaborative Voluntary Partnerships: Lessons from the Federal Aviation Administration by Russell W. Mills

Strategies for Supporting Frontline Collaboration: Lessons from Stewardship Contracting by Cassandra Moseley

Food Safety—Gaps and Emerging Public-Private Approaches: A Perspective for Local, State, and Federal Government Leaders by Noel P. Greis and Monica L. Nogueira

Conserving Energy and the Environment

A Guide for Local Government Executives on Energy Efficiency and Sustainability by Nathan Francis and Richard C. Feiock

Fostering Transparency and Democracy

Using Geographic Information Systems to Increase Citizen Engagement by Sukumar Ganapati

REPORTS from

The IBM Center for The Business of Government

Improving Performance

Project Management in Government: An Introduction to Earned Value Management (EVM) by Young Hoon Kwak and Frank T. Anbari

Strategic Use of Analytics in Government by Thomas H. Davenport

Managing Finances

Managing Risk in Government: An Introduction to Enterprise Risk Management (2nd Edition) by Karen Hardy

Strengthening Cybersecurity

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers by Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams

Transforming the Workforce

Engaging a Multi-Generational Workforce: Practical Advice for Government Managers by Susan Hannam and Bonni Yordi

Implementing Telework: Lessons Learned from Four Federal Agencies by Scott P. Overmyer

Using Technology

An Open Government Implementation Model: Moving to Increased Public Engagement by Gwanhoo Lee and Young Hoon Kwak

How Federal Agencies Can Effectively Manage Records Created Using New Social Media Tools by Patricia C. Franks

About The IBM Center for the Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:

Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342
website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com
twitter: twitter.com/busofgovernment

Stay connected with the IBM Center on:

f govloop
in t
You Tube™

or, send us your name and e-mail to receive our newsletters.