15/2

Volume 15 Number 2 • **Spring 2012**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Social Media Malware

also inside

IATAC

contents

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Assistant Secretary of Defense for Research & Engineering ASD(R&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or ASD(R&E). The mention of commercial products does not imply endorsement by DoD or ASD(R&E).

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director: Gene Tyler
Inquiry Services: Karen Goertzel

If you are interested in contacting an author directly, please e-mail us at *iatac@dtic.mil*.

***IAnewsletter* Staff**

Chief Editor	Gene Tyler
Assistant Editor	Kristin Evans
Art Director:	Tammy Black
Copy Editor:	Alexandra Sveum
Editorial Board:	Al Arnold
	Angela Orebaugh
Designer:	Tammy Black
	Dustin Hurt

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit *http://iac.dtic.mil/iatac/IA_newsletter.jsp* and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/ Additions/Deletions**
To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

E-mail: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*

Cover design: Tammy Black
Newsletter design: Donald Rowe

Distribution Statement A: Approved for public release; distribution is unlimited.

Editors Picks

Video President Obama recognizes the paradox cyberspace creates (Source: *http://www.youtube.com/watch?v=jemkAu-zpms&feature=related*)

Video DoD remains focused on developing its cybersecurity (Source: *http://www.youtube.com/watch?v=qvYc0KEMilQ*)

Video Former Director of National Intelligence and current Vice Chairman of Booz Allen Hamilton, Mike McConnell, discusses the importance of securing our cyber infrastructure (Source: *http://www.youtube.com/watch?v=c2wP6vRjra0&feature=related*)

Video This video presents general facts about social media and its impact on the world today (Source: *http://www.youtube.com/watch?v=ZQzsQkMFgHE&feature=related*)

Video With the help of technology, our world is changing rapidly. (Source: *http://www.youtube.com/watch?v=ljbI-363A2Q*)

We would like to introduce you to our first ever virtual edition of the *IAnewsletter*. This edition continues our long-standing tradition of presenting cutting-edge articles by information assurance (IA) and cybersecurity subject matter experts from across government, industry, and academia.

By going virtual, we can also link you to a variety of online articles and references, thought-provoking video clips, and online forums that are helping to change the way we approach IA as future technologies—and threats—emerge.

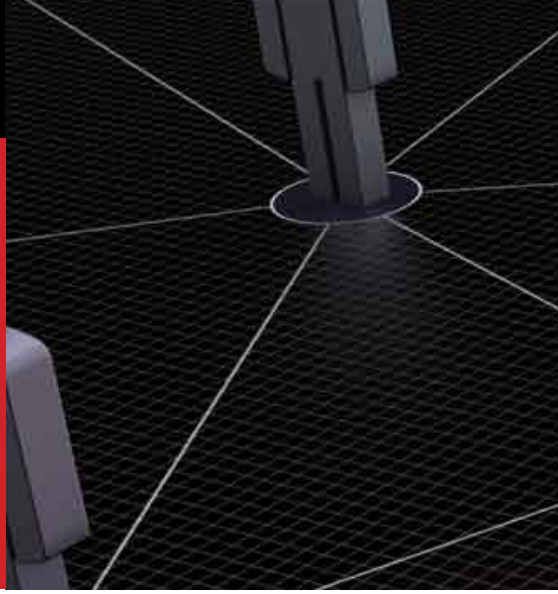
We hope you discover that receiving the *IAnewsletter* provides you not only with a collection of interesting articles, but also with an interactive experience connecting you more fully with what is happening in IA and cybersecurity online and in our world.

So sit back and enjoy! Let our virtual *IAnewsletter* take you on a ride.

—The *IAnewsletter* Editorial Board

Social Media Malware

by Angela Orebaugh



Social networking is continuing to reinvent how users consume, view, and share information as millions of users are now using some form of social media. As social media platforms become more prevalent, their security threats, attacks, and malware continue to grow as cybercriminals take advantage of the implied trust relationships inherent in social networking. Popular platforms, such as Facebook and Twitter, have become targets for attackers, spammers, and other cybercriminals looking for easy victims, making social media the top delivery vehicle for malware. Facebook now has over 500 million active members, making it very attractive for cybercriminals to reach a large number of potential victims. The many-to-many relationship model of social media allows malware to spread rapidly and exponentially. Social media malware may install malicious software on a victim's computer and trick victims into revealing information (*e.g.*, credit card information, bank information, and other personal data used for identity theft), or trick users into completing unnecessary surveys that earn the cybercriminal affiliate advertising revenue. The combination of social media platform features and users' behaviors provide increasing avenues of attack for malicious software and activities. Popular attacks include—

The many-to-many relationship model of social media allows malware to spread rapidly and exponentially.

- **Clickjacking**—Malicious hidden actions are performed when a user clicks a visible button or link. This type of malware uses embedded code that executes without the user's knowledge.
- **Drive-by Downloads**—Malware is automatically downloaded to a victim's computer without his/her knowledge or consent when visiting a malicious Web site.
- **Password Compromise**—Cybercrimals compromise passwords by presenting the user with a fake log-in page or by requesting username and password information in malicious social media apps.

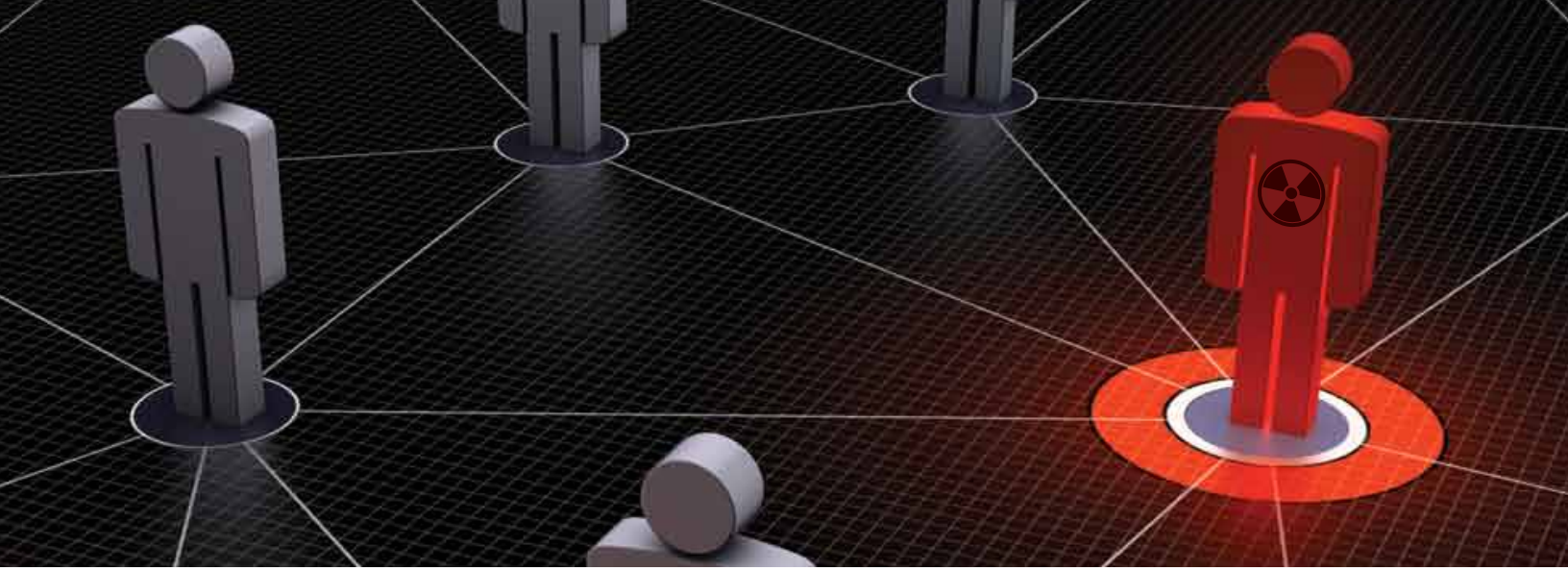
Cybercriminals may use the attack vectors described below to propagate malware:

Direct Messages—Attackers may spoof users' friends or popular entities and send personalized messages to entice them to click malicious links or reveal personal information.

Malicious Content—Wall posts, tweets, and other social media public message mediums may contain enticing

Facebook Malware Examples

- A recent example of Facebook malware was the Valentines Day theme. The attack spread by wall posts that invite users to install a Valentines Day theme for their Facebook profile. The link in the post redirects the victim to a Web page to install the "theme," which actually installs malware that displays ads, installs a Web browser extension that monitors Web activities, and redirects sessions to survey pages that request sensitive information such as phone numbers. [1]
- Another example was the exploitation of Whitney Houston's death with a link to a supposed video of her autopsy on Facebook. The link led victims to survey scams and malware. [2]
- Likejacking is a clickjacking attack that tricks users into clicking a link that marks a Facebook page as "Liked," and shows up on the victim's profile and wall, which then entices friends to also click the link. The page "Likes" often result in ad affiliate revenue for the cybercriminal likejacker.
- The Stalk my Profile scam has dozens of variations, and lures victims by falsely offering to show users who have viewed their profile. The scam generates ad affiliate revenue for cybercriminals as users click through the process of trying to obtain the app.
- The Facebook Dislike button scam made several rounds over the years with many variations. All of the scams offered to add a new Dislike button feature to the user's profile; instead, it attempted to install malware. [3]



posts, such as free gift cards, links to videos of significant events, false advertisements for applications, fake security issues, and celebrity gossip. These malicious posts often appear on infected accounts as a way of propagating the malware. Malware may also appear in malicious advertisements; these are called malvertisements. Malvertisements cause problems for both users and legitimate advertisers because fake or compromised advertising sites put users at the risk of being phished or scammed and legitimate advertisers lose money and customers to spoofed sites. For example, a common attack is the survey scam that lures users to complete a survey prior to receiving a free gift card (often Starbucks). Each survey that is completed earns the scammer affiliate advertising money, and the victims never receive the reward. Facebook recently filed a lawsuit against Adscend Media LLC, alleging the company spread malware and stole personal information through advertising links. The suit claims that Adscend was aware of and encouraged its affiliates to engage in activity that directed users to bait pages with surveys, where the affiliates were paid each time a user took a survey. [4]

Shortened URLs—Wall posts, direct messages, tweets, and other social media messages may include URLs that have been given a shortened alias. This is a long-standing, but still effective, method for attackers to lure victims to malicious sites. Facebook has implemented URL checking software, but not all social media platforms offer this type of service.

Malicious Apps—Clicking malicious links may install malicious apps by asking users to upgrade their Flash player, or by installing a fake security software application. Apps may also request access to more personal information than necessary. They may also request your username and password.

Fake Profiles—Cybercriminals create fake social media profiles to post enticing malicious content and send direct messages.

E-mail—Some cybercriminals attempt to send malware or phishing scams *via* e-mail messages that look like legitimate social media friend requests, notifications, or other messages from a specific social media platform.

Social networking sites are starting to employ security measures to protect against some malware on their platforms. In January 2012, Twitter announced its acquisition of spam and malware service, Dansient, which is a company that offers a Web anti-malware platform capable of scanning URLs and Web sites for malicious content; however, with billions of posts, tweets, ads, and other messages being sent across social networking sites each day, it is hard for providers to keep up with all scams and malware.

Twitter Malware Examples

- A continuing Twitter malware propagation technique uses trending topics to create fake tweets that include the name of a trending topic in hopes to get a high number of victims to click the malicious link.
- In 2010, Twitter was infected by a mouseover exploit that triggered a pop-up ad malware worm to launch when a user moved his mouse over the malicious tweet. [5]
- Twitter has been infected with fake anti-virus scams that tell the user they have a virus and need to download an anti-virus program in the provided link. Some victims fall for this scam by paying $89 for fake anti-virus software. [6]

Koobface

The most notable social media malware is Koobface, a worm that targeted many social networking platforms and infected a variety of operating systems including Windows, Mac OS X, and Linux. The worm gathers log-in information for social media platforms and uses the compromised computers to build a botnet. It originally spread wildly on Facebook in 2008 through infected friends by offering a wall post for an enticing (fake) video via a shortened URL that redirects to a malicious site. When a user clicks the video link, he/she is provided a link to update his Adobe Flash plug-in, which instead installs malware on the victims computer. Over the years, there have been a number of variants of Koobface, including some that use other delivery mediums, such as direct messaging. [7]

Video Social Media Malware is discussed at RSA Conference 2010 (Source: *http://www.youtube.com/watch?v=Fzyquo7Y2Vs*) *The IAnewsletter does not endorse any products mentioned.*

As a responsible user, you can stop malware in its tracks.

As a responsible user, you can stop malware in its tracks and end the exponential propagation in social media platforms by employing a few simple security measures—

- Think before you click. Often with social media, users implicitly trust messages and posts from their networking contacts and friends. Scrutinize everything!
- If a social media friend posts or sends a message that is out of character, assume his account was compromised and scrutinize the content cautiously.
- Do not automatically trust notifications that sound sensational or too good to be true, such as free gift cards or revealing videos. The upcoming 2012 Olympics, for example, are sure to be a target for social media malware campaigns.
- Scrutinize vague direct messages with comments such as "check out this video I found of you."
- Install a browser add-on to help protect against malware. For example, the NoScript plug-in for Firefox alerts you when scripts are loaded from external pages.
- Check the URL bar in your browser when installing Facebook apps to make sure the link is really for Facebook.
- Scrutinize apps that ask for your username and password.
- Avoid downloading software from unknown sites.
- Keep your operating system, browser, and other applications patched and your anti-virus software updated.
- Do not click links in e-mails that include social media friend requests, notifications, or other messages. Log in to your social media account to verify requests and messages.
- Beware of messages claiming to install new features that are not currently available on your social media platform, such as the Facebook Dislike button or the "see who viewed your profile" apps.
- Avoid surveys on social media platforms; they are often scams.
- Use a URL decoder to verify shortened links, such as *TrueURL.net*.
- Do not open e-mails or messages received on social networks from unknown senders.
- Do not use the same password across multiple accounts. ■

About the Author

Angela Orebaugh | is a technologist, researcher, and cybersecurity executive, who is passionate about helping clients embrace tomorrow's technology today. Ms. Orebaugh was recently selected as Booz Allen Hamilton's first and currently only Cyber Fellow, a distinction reserved for an elite group of the firm's most noted authorities. She evangelizes social media and mobile technologies by highlighting the powerful ways in which these technologies are changing business, communications, and information sharing. Ms. Orebaugh is also the Information Assurance Technology Analysis Center Director of Research and Academic Integration. She is an international author and invited speaker for technology and security events. Follow her on Twitter *@AngelaOrebaugh* and connect with her on Google+ at *http://gplus.to/angelaorebaugh*. She can be contacted at *iatac@dtic.mil*.

References

1. *http://www.prweb.com/releases/2012/2/prweb9178582.htm*
2. *http://www.gmanetwork.com/news/story/248294/scitech/socialmedia/whitney-houston-autopsy-scam-video-on-facebook*
3. *http://securitywatch.pcmag.com/security-software/283476-beware-the-facebook-dislike-button-scam*
4. *http://www.scmagazine.com/facebook-sues-adscend-media-for-malware-and-spam/article/225344/*
5. *http://nakedsecurity.sophos.com/2010/09/21/twitter-onmouseover-security-flaw-widely-exploited/*
6. *http://www.pcworld.com/article/217308/twitter_targeted_with_fake_antivirus_software_scam.html*
7. *http://www.thatsnonsense.com/viewdef.php?article=koobface_virus*

Angela Orebaugh

by Kristin Evans

The *IAnewsletter* profiles a member of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program in each edition. IATAC's Director of Research and Academic Integration, Angela Orebaugh, authors these profiles. This article highlights Ms. Orebaugh's contributions in building IATAC's relationships with academia and her overall contributions to information assurance (IA) and cybersecurity.

Ms. Orebaugh is completing her Ph.D. in Information Technology with a concentration in Information Security at George Mason University, where she is also an adjunct professor. She instructs courses on intrusion detection based on curriculum she developed for the Computer Forensics certificate offered by George Mason's Department of Electrical and Computer Engineering. Ms. Orebaugh also helped create the curriculum for the new M.S. degree in the Computer Forensics program. She earned her M.S. degree in Computer Science and B.S degree in Computer Information Systems from James Madison University.

As IATAC's Director of Research and Academic Integration, Ms. Orebaugh has been integral in promoting collaboration across government, industry, and academia. She was the Cybercrime Investigations Track Chair for the 2009 International Conference on Digital Forensics & Cyber Crime, and she delivered the keynote address at the University of Virginia Local Support Partners Conference in 2008. She has also been an invited speaker at several technology-focused conferences, including the System Administration, Networking, and Security (SANS) Institute and Institute for Applied Network Security. Additionally, Ms. Orebaugh serves as an Advisory Board member for CyberWatch Center, a consortium of community colleges and universities across 28 states that share best practices and training methodologies in efforts to funnel highly trained professionals into the IA workforce. [1]

Perhaps Ms. Orebaugh's greatest contributions are her publications as a result of her diverse IA and cybersecurity research interests. Her research interests span intrusion detection and prevention, packet analysis, vulnerability management, data mining, attacker profiling, user behavior analysis, behavioral biometrics, cyber psychology, network forensics, and cybercrime. She has authored six books (*Nmap in the Enterprise, How to Cheat at Configuring Open Source Security Tools, Wireshark & Ethereal Network Protocol Analyzer Toolkit, Snort Cookbook, Intrusion Prevention and Active Response: Deploying Network and Host IPS,* and *Ethereal Packet Sniffing*), several papers for peer-reviewed journals, and a number of magazine articles. Ms. Orebaugh is a strong advocate for social media and mobile technologies, writing several articles on these topics for the *IAnewsletter* including, "Social Networking and Privacy," "Securing the Mobile Device…and its User," "Identifying and Characterizing Instant Messaging Authors for Cyber Forensics," and in this edition, "Social Media and Malware."

In addition to books, papers, and articles, Ms. Orebaugh has helped develop cybersecurity strategy at the National Institute of Standards and Technology as a senior leader at Booz Allen Hamilton. Through her consulting engagements, she has contributed to industry standards development and several regulatory papers for the National Vulnerability Database and Security Automation Program. Recently, Booz Allen named Ms. Orebaugh its first Cybersecurity Fellow as a part of its Functional Skills Belting Program. [2] This designation recognizes her contributions to IA and cybersecurity across the government, industry, and academia over her 18-year career. [3] ■

References

1. http://www.cyberwatchcenter.org/
2. http://www.boozallen.com/media-center/press-releases/48399320/angela-orebaugh-fellow
3. http://securityknox.com/about/

Damages from Cyber Attacks by Attack Category and Damage Type

by Soumyo D. Moitra

In spite of all the network security precautions that organizations take, we know that inevitably some cyber attacks can get through and cause damage. Information assurance (IA) and network security managers would like to know what the impacts of such attacks are on their systems. While there are now many sources of information on reported damage from cybercrimes, the data are often not useful for making security decisions at the organizational level. This article presents data from a survey of experienced professionals, asking them to estimate the extent of such damages by Attack Category and Damage Types. This article presents the results to allow security managers to use this information as reference values for their own analysis. Also, the methodology to collect the data can be replicated by individual organizations to assess their own situations.

A previous *IAnewsletter* article described a model for estimating the benefits from network security systems [1]; however, the application of the model required specific data and gathering that data was one of the challenges, which is where illustrative values were used instead. This article reports the results of a survey that is designed and conducted to collect some of that data. In particular, this article reports the ratings of damages from cyber attacks as elicited from the survey respondents. This data is essential as input for that model, but not generally available otherwise.

Why Do We Need Data on the Impacts of Cyber Attacks?

The genesis of this work was a real need to evaluate the benefits from investment in network security. To estimate these benefits, it is necessary to know what the expected damage would be with and without the security system in place. The benefits then would be the expected reduction in damages. While there might be other benefits, this damage reduction was the focus of this work. All cost-benefit models for network and information security, such as ALE (Annualized Loss Expectancy), ROI/ROSI (Return on Investment/Security investment), NPV (Net Present Value), *etc.*, require this information [2, 3, 4, 5, 6]; therefore, for effective security-related decisions, it is important to first know the expected damage that cyber attacks might cause.

Additionally, for situational awareness, it is important for security managers to know the risks their organization face from cyber attacks. One of the elements of risk assessment is an understanding of the potential damage from cyber attacks. The knowledge of their impact is essential for security policymaking and planning. [7, 8, 9, 10]

Such data, though crucial and much needed, are currently not easily available in the public domain. There are at least three reasons for this—

- the data has generally not been collected in the past;
- the data can be difficult to collect without having a standard methodology in place; or
- the reluctance of organizations to publicly admit to such losses.

While a number of surveys and reports are now available that attempt to estimate damage from cyber attacks and cybercrimes, they are not very useful for managerial decision making since, among other reasons, the estimates are aggregated over specific samples and would not apply to a specific organization. [11, 12, 13]

Data collection and analysis from security surveys is complex, and a variety of errors can arise. In any case, experts would need to validate them. Often, eliciting estimates directly from experts can actually lead to quite reliable assessments [14]; however, these estimates can only be useful if obtained from experts, but it is normally very difficult to find such experts and elicit their opinions. This is yet another reason why estimates of damage are rare in open literature. A general survey will not yield accurate results as this area is highly specialized.

Estimating the Impacts of Cyber Attacks: What the Experts Think

A survey was fielded to a focus group of experienced security analysts that asked them to rate the expected damage from successful cyber attacks. A key and novel feature of the question was that it asked for damage ratings by Attack Category and Damage Types. This disaggregation is extremely important since different attacks will have different impacts and the impacts of any attack will affect different components of the network system differently. For example, the damage to hardware will generally be different from the damage to communications, and both will be different from damage due to data loss.

In our analysis, we have distinguished between Attack Categories and Damage Types, and have constructed an Attack/Damage matrix that is shown in Table 1. Five categories of attacks were chosen based on those used by the Department of Defense (DoD)—

1. Root Level
2. User Level
3. Denial-of-Service (DoS)/ Distributed DOS (DDos)
4. Malware
5. Data Exfiltration.

Six sources of damage were distinguished—

1. Hardware
2. Software
3. Communications
4. Operations
5. Data
6. Sensitive Information.

Attacks impact these sources of damage differently, and we need to know the Damage Type for each Attack Category. Another novelty here is the distinction between "data" and "sensitive information." By "data," we mean information that is not controlled, such as information available in the public domain or archival data that would not be of any use to an adversary. By "sensitive information," we mean all controlled information that the organization possesses, protects, and does not wish unauthorized entities to access. This is particularly important for the DoD and other organizations with valuable, proprietary informational assets.

The sample size is small (12 completed responses), but the responses are valuable because they are from knowledgeable professionals. The results, therefore, may be considered as data from a focus group of experts. We elicited estimates of relative damages on a scale from 0 (no damage) to 100 (maximum possible damage). While similar information is available in the public domain, it is highly scattered and has not been systematically presented in this form.

How Much Damage Might be Caused?

Table 1 and Table 2 summarize the results of the survey. There were five Attack Categories and six sources of potential damage (explained above); therefore, there are 30 cells in each table. In addition to examining the means and medians, we should note that there was a considerable divergence among individual estimates, which could arise for a variety of reasons: different implicit assumptions made by the respondents, different experiences in different organizations, or different interpretations of values on the scale of 0 to 100. As we shall see, however, the means and medians seem reasonable and appear to match what we might expect and can interpret.

Table 1 shows the three highest-rated damages were for communications losses from exfiltration of sensitive information, and losses to operations capabilities under DoS/DDoS attacks. These clearly appear reasonable, as the consequences of these attacks are known to be severe. Loss of communications and operations capabilities could endanger the lives of personnel in active duty and support functions, and would have a cascade of other serious consequences. Loss of sensitive data could also be very serious for data such as information on weapons systems.

Most of the ratings were around the middle of the scale, and the grand

Attack Category	Source of Damage from a Cyber Attack					
	Hardware	Software	Communications	Operations	Data	Sensitive Information
Root Level	26	57	50	70	73	78
User Level	15	22	35	53	53	58
DoS/DDoS	25	27	87	84	17	14
Malware	26	58	48	51	69	70
Data Exfiltration	5	15	18	35	75	85

Table 1 Mean rating of expected damage by the source of that damage and by attack category

Attack Category	Source of Damage from a Cyber Attack					
	Hardware	Software	Communications	Operations	Data	Sensitive Information
Root Level	10	60	45	75	90	90
User Level	2.5	12.5	25	55	50	55
DoS/DDoS	10	10	90	90	10	5
Malware	15	65	50	50	75	80
Data Exfiltration	0	0	2.5	30	85	94.5

Table 2 Medians of ratings of expected damage by the source of that damage and by attack category

average was 46. The responses generally show an awareness of what attacks would cause what damages, appearing to be fairly reliable in spite of the diversity of individual estimates. The four lowest ratings were for damages to hardware and software from data exfiltration exploits, to hardware from user level attacks, and to sensitive information from DoS/DDoS attacks. Again, they appear to be quite reasonable. The responses covered the full spectrum of the 0 to 100 scale and did not cluster around any particular rating. Two cases where the spread was relatively narrow were for—

- Damages to Communications from DoD/DDoS Attacks—100 to 70 only
- Damages to Hardware from Data Exfiltration Attacks—50 to 0 only.

This result indicates that there was a consensus that the first case was serious and the second was not very serious.

Given the diversity of estimates, it would be useful to analyze the data after excluding the effect of outliers or extremes. This can be done by looking at the medians since they measure the central point of an array of values. The median is the middle value after the responses are ordered; half the values will be above it and half below. Outliers, therefore, will have no effect on the median; whereas, they affect the mean since the mean is computed from the average of all values. Table 2 displays the medians. Among the highest values, three are the same as those seen when analyzing the means: communications losses from DoS/DDoS, losses from exfiltration of sensitive information, and losses to operations capabilities under DoS/DDoS attacks. Four new cells, however, appear to have high medians: data and sensitive information losses from root level attacks, data losses due to data exfiltration, and loss of sensitive information due to malware. All of these findings can be interpreted easily. Most respondents thought that root level attacks could result in losses of data and sensitive information. This is quite understandable, although a few respondents rated these losses very low, which is why the means were not very high. The other two findings (data losses due to data exfiltration and loss of sensitive information due to malware) can be interpreted the same way.

At the low end, most respondents thought that there would be no losses to hardware and software as a result of data exfiltration. They expected very low losses to communications from data exfiltration, to hardware from user level attacks, and to sensitive information from DoS/DDoS attacks. All these cells are the same ones noted when looking at the means.

Overall, we find that respondents identified some specific damages as particularly high, some particularly low, and both the results have reasonable explanations. We also find that the results from examining the means are broadly similar to the results from the medians.

Summary

This paper analyzes the results of a survey where network security professionals were asked to estimate the damages that might be caused by cyber attacks. They were asked to rate the damages by Attack Category and Damage Type on a scale of 0 to 100. The findings indicate that the respondents attributed the most serious damages to—

- Loss of Sensitive Information from Data Exfiltration Attacks
- Loss of Communications Abilities from DoS/DDoS Attacks

- Loss of Operations Abilities from DoS/DDoS Attacks
- Loss of Data from Root Level Attacks
- Loss of Sensitive Information from Root Level Attacks
- Loss of Sensitive Information from Malware Attacks.

They estimated the least damages were due to—

- Hardware Losses from Data Exfiltration Attacks
- Software Losses from Data Exfiltration Attacks
- Loss of Communications Abilities from Data Exfiltration Attacks
- Hardware Losses from User Level Attacks.

These findings are exploratory in nature and should be treated as preliminary because of the small sample size; therefore, no detailed statistical analysis was done. Such responses from knowledgeable practitioners, however, are valuable in and of themselves because it is otherwise difficult to obtain such a perspective.

Conclusions and Discussion: Understanding the Risks

The following points highlight key considerations for organizations investing in cyber attack prevention—

- This article has presented data on relative damages that cyber attacks could cause, which is the input needed to estimate the benefits from network security systems as described in a previous article in the *IAnewsletter*. [15]
- Even if an organization does not use the data for cost-benefit analysis (perhaps because of reservations about its validity [16, 17]), the data are still important for network situational awareness and organizational strategic planning for security.
- This article has illustrated a method to quantify these damages. This method is relatively simple, can be done quickly, and can be repeated regularly to keep the information up to date. Managers could also use the results as benchmarks to assess their own security.
- The attack/damage matrix can be estimated at two levels: with and without security controls. The difference indicates the degree of mitigation that the organization might be expected to achieve.
- In the past, managers have found it difficult to apply cost-benefit models to information security and not used them. This information is also not readily available or is difficult to collect; however, this is widely recommended. [18] Now it should be easier for managers to use such models. This analysis fulfills a need for this data, and the results provide quantitative insights into potential vulnerabilities by highlighting the damage that might occur from cyber attacks. The work reported here was part of a larger project at the Network Situational Awareness group at CERT. [19]
- Using a scale to elicit relative estimates of damages makes the results more general. Organizations can calibrate the values as appropriate for them and can arrive at cost-values if they wish. These cost-values can be used for cost-benefit analysis, if desired. Additional data will be needed, including the rate of cyber attacks that the organization experiences.
- The attack/damage matrix is a very useful model, and the analysis showed that disaggregating Attack Categories and Damage Types provides significant insights into the network risks that the organization might face.
- The matrix is best estimated at the organizational level with respect to a network under the same controls and policies, and one that is protected by a coordinated security system.

Future Challenges: Getting to the Next Level

The following points should be considered for advancing the state of IA with respect to cyber attack prevention—

- It is important to conduct additional confirmatory investigations of cyber attacks. We need more and larger surveys to validate the findings reported here. Also, the Attack Categories and Damage Types could be expanded.
- For organization-specific security decisions, surveys should be fielded to individuals familiar with the organization, the threats it faces, and its informational assets. Organizations need to update this information on damages as conditions can change quickly and regular updating is important. The survey could be modified to elicit cost-values; however, in that case, care needs to be taken to reduce possible errors and biases to maintain reliable results.
- It would be useful to actually use the data in cost-benefit models, which requires appropriate socialization among the stakeholders in the organizations and perhaps beyond. In applying the data to models, careful analysis needs to be conducted to ensure that the assumptions are met before results are used in decisions.

This article presents some results from an open survey and the author's description of them. Opinions that may be expressed here do not necessarily represent the opinions of CERT, the SEI, or Carnegie Mellon University. ■

About the Author

Soumyo Moitra | is a Senior Member of Technical Staff in the CERT Network Situational Awareness Group at the Software Engineering

▷ ▷ *continued on page 39*

Responsible Information Sharing I: Responsibility to Share

by Karen Mercedes Goertzel

This is the first article in a two-part series that highlights the need to share information on one hand, and the need to protect it on the other. The hyperlinks throughout this article provide you quick access to additional information.

Background: The Imperative to Share

The tragic events on September 11, 2001 spurred the United States to re-evaluate its defense, intelligence, and law enforcement priorities and structures. This article highlights the information sharing initiatives that resulted from lessons learned in the aftermath of these terrorist attacks. Lessons learned after 9/11 led to the enactment of a series of laws, directives, and executive orders (EOs) that collectively established a new culture and new policies, mechanisms, and governance for improved sharing of homeland security, terrorist, and weapons of mass destruction information among federal agencies and state, tribal, and local governments; the private sector; and foreign partners.

The President's first action after 9/11 was the issuance of the *Homeland Security Presidential Directive (HSPD)-7* on December 17, 2003 to expand the scope of critical infrastructure. HSPD-7 called for facilitated sharing of terrorism-related information among government agencies with the supporting EO 13311, *Homeland Security Information Sharing* (July 29, 2003), designating various department heads to executive functions/ responsibilities for implementing the improved information sharing mandate within and beyond the federal government, and for determining with which non-federal entities classified national security information could and should be shared.

The Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission) then published its July 2004 report, which identified specific gaps in federal, state, and local government information sharing capabilities as contributing factors in the government's failure to prevent the 9/11 attacks.

In response, the President issued EO 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans* in August 2004, which was revised and superseded by EO 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* in October 2005. They mandate that federal departments and agencies shall give highest priority, with regard to information system design and information dissemination, to "the interchange of terrorism information among agencies" and "between agencies and appropriate authorities of state, local, and tribal governments, and between agencies and appropriate private sector entities" as well as "the protection of the ability of agencies to acquire additional such information." EO 13388 also established an Information Sharing Council composed of representatives of key departments and agencies to make information sharing a priority across the federal government.

Figure 1 *National Strategy for Information Sharing* and *Information Sharing Environment Enterprise Architecture Framework*

In December 2005, the President followed up EO 13388 by issuing a memorandum to kick off the government-wide Information Sharing Environment (ISE). The *ISE Implementation Plan* was published in November 2006. Interestingly, information security/assurance per se was not called out as a major challenge, although the implementation plan discusses the challenges of implementing personnel security and certification and accreditation in the context of handling classified terrorism information within the ISE. Not until ISE Version 2, published in September 2008,

did the ISE address information security and assurance (Chapter 4).

To more clearly delineate national information sharing objectives, the White House issued *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Terrorism Information Sharing* on October 31, 2007, outlining objectives for improving the sharing of information pertaining to homeland security, terrorism, and law enforcement related to terrorism (1) at the federal level (*e.g.*, among departments/agencies); (2) between federal and state, local, and tribal entities; (3) between federal and private sectors; and (4) between U.S. entities and foreign partners. All information sharing is to be consistent with imperatives to protect the privacy, civil rights, and other rights of parties engaged in sharing, and parties about whom information is shared. The ISE's role as an enabler for establishing trusted information sharing partnerships is also clarified.

As part of the ISE initiative, the White House established an Information Sharing and Access Interagency Policy Committee (ISA IPC) in July 2009. The ISA IPC chartered various working groups and subcommittees to address security and privacy issues in interagency and external information sharing.

To date, ISE's main objective has been achieving interoperability between the sensitive but unclassified (SBU)/controlled unclassified information (CUI) networks of ISE-participating departments and agencies. To achieve this goal, ISE has focused on implementing Simplified Sign-On (SSO) to enable law enforcement's online users to access defense, civilian, and law enforcement SBU/CUI intelligence networks and systems, such as Intelink-U and the Regional Information Sharing Systems Network.

According to the Government Accountability Office's July 2011 report, *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*, while the ISE Enterprise Architecture Framework and associated documents define mechanisms for identity and access management and information system trustworthiness, they do not explain how current mechanisms/controls can be leveraged to assure information confidentiality, integrity, and availability. They also do not provide a transition plan for moving from existing security mechanisms/controls to future ISE Information Protection/Assurance business processes. Finally, the documents lack mechanism for defining controls to segregate data into different security domains.

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) was amended by Title V of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53). Entitled *Improving Intelligence and Information Sharing within the Federal Government and with State, Local, and Tribal Governments*, Title V's mandates that are most salient for the security and privacy of information shared *via* the ISE included—

- The ISE must provide a process by which authorized officials can change information access, use, and retention policies for the ISE.
- The ISE must incorporate "continuous, real-time, and immutable audit capabilities, to the maximum extent practicable."
- The President must determine and report to designated House and Senate committees on the feasibility of—
  - Eliminating explicitly exclusionary information markings and processes;
  - Replacing exclusionary markings/processes with Authorized Use standards; and
  - Allowing information owners, handlers, collectors, and disseminators to provide "anonymized data."

Title V of the 2007 Act also revised language in the IRTPA regarding privacy and civil liberties protections in

connection with ISE and information sharing, while Title XII, Transportation Security Planning and Information Sharing, amended some security/privacy-relevant elements of earlier legislation, most notably in calling for expediting of security clearances for public and private stakeholders to enable them to access classified transportation security information. Title XII includes the further provision that whenever possible, transportation security information is provided to such stakeholders "in an unclassified format."

Since 2007, a number of other Presidential EOs have been issued to clarify various aspects of the security and privacy elements of government information sharing initiatives and the ISE, including—

- **EO 13467**—*Reforming Processes Related to Suitability for Government, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (June 30, 2008) calls for ensuring "an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for government employment, contractor employee fitness, and eligibility for access to classified information," while not unjustifiably inhibiting the information sharing mandated by Title III of the 2004 IRTPA.
- **EO 13526**—*Classified National Security Information* (December 29, 2009) "prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism."
- **EO 13549**—*Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities* (August 2010) "delineates rules and measures required for the proper safeguarding of classified information to be shared with state, local, tribal, and private sector entities."
- **EO 13556**—*Controlled Unclassified Information* (November 4, 2010) establishes a program, to be administered by the National Archives and Records Administration (NARA), to manage all unclassified information that requires safeguarding and/or dissemination controls required by and consistent with applicable law, regulations, and government-wide policies. In June 2011, NARA's CUI Office issued the "Initial Implementation Guidance for Executive Order 13556."
- **EO 13587**—*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (October 7, 2011) further delineates rules and measures, informed by lessons learned from the WikiLeaks disclosures, for "the responsible sharing and safeguarding of classified national security information on computer networks."

Figure 2 Global information sharing

In May 2010, the White House also issued its *National Security Strategy*, which reinforces the implementation and leveraging of information sharing as a means to improve the gathering and use of intelligence.

The federal government was not the only government entity that advocated for changes in how information should be shared; the following sections highlight information sharing initiatives across the government, including international initiatives.

Information Sharing in DoD

The DoD issued its Directive *Data Sharing in a Net-Centric Department of Defense* (DODD 8320.02, December 2,2004; recertified April 23, 2007), which states as DoD policy that "data assets shall be made accessible by making data available in shared spaces." The policy also describes how security metadata tagging will be used to assure consumers of DoD information of its trustworthiness.

The *DoD Information Sharing Strategy* (May 4, 2007) "guides…sharing of information within the DoD, and with federal, state, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental

organizations, and the private sector." The near-term tasks intended to move DoD closer to implementing information as envisioned in the strategy are described in the *DoD Information Sharing Implementation Plan* (April 2009).

Other DoD information sharing initiatives include—

- **Multi-National Information Sharing**—Intended to facilitate information sharing among DoD components and eligible foreign nations in support of planning and execution of military operations.
- **All Partners Access Network**—A DoD enterprise-level unclassified information sharing program to enable information exchange and collaboration between DoD and foreign countries, organizations, and individuals who do not have access to traditional DoD systems and networks.

Intelligence Community Information Sharing

Anticipating DoD by 6 months, the Director of Central Intelligence issued his Directive, DCID 8/1, *Intelligence Community Policy on Intelligence Information Sharing,* in June 2004. Among other policy elements, DCID 8/1 calls for increasing the production of intelligence that can be shared at multiple security levels and defining methods that can be used to achieve this. The DCID also calls for Intelligence Community (IC) entities to adopt standards and IT systems "that support secure sharing of intelligence information within the community and with customers."

To address some of the information sharing gaps identified in the *9/11 Commission Report,* the President established an Interagency Threat Assessment and Coordination Group (ITACG) within the National Counterterrorism Center. The ITACG (codified into law by Congress) was assigned the mission of improving information sharing between the National Counterterrorism Center and state, local, and tribal governments. To do this, it has undertaken the identification of national intelligence products that may be of use to state/local/tribal consumers, suggested edits that would render these products more useful to those consumers, and generally advocated within the IC to ensure that state/local/tribal terrorist information needs are satisfied.

Another Congressional response to the *9/11 Commission Report* was the enactment of the *IRTPA of 2004* (Public Law 108-458). Section 1016 of the IRTPA mandates the establishment of ISEs as enablers for interagency sharing of terrorism-related information.

As the *DoD Information Sharing Strategy* does for DoD, the *United States Intelligence Community Information Sharing Strategy* (February 22, 2008) defines a strategy for the IC that will enable it to establish a new culture of information sharing "and to share information better, both among those whose job it is to provide intelligence and with those who need intelligence to perform their missions."

In the spirit of cooperation engendered by the various information EOs and sharing policies under which they now operate, with the issuance in July 2006 of a joint DoD Chief Information Officer (CIO)/IC CIO Memorandum, *Establishment of a DoD/IC Unified Cross Domain Management Office (CDMO),* DoD and the IC aligned their cross-domain information sharing oversight and governance efforts under a single Unified CDMO. Five years later, DoD's CIO issued a memorandum on Cross Domain Support Element responsibilities that further clarified the DoD's responsibilities in support of the CDMO efforts. [1]

Homeland Security Information Sharing

The Department of Homeland Security (DHS) is, in many ways, the most active proponent and implementer of information sharing within and beyond the federal government. Among its *numerous initiatives* are the Homeland Security Information Network and National Terrorism Advisory System, the Homeland Security Operation Center, DHS terrorism monitoring MegaCenters and intelligence Fusion Centers, and the Information Sharing Fellows Program, as well as the information sharing initiatives of its various subsidiary components and offices.

DHS also established an *Intelligence, Security, and Information Section* to help its components/offices "ensure that civil rights and civil liberties protections are incorporated into the Department's information and physical security programs, information sharing activities, and intelligence-related programs and products." To achieve this oversight for information sharing, the section coordinates its efforts with the DHS Information Sharing and Coordination Council and Information Sharing Governance Board. Its efforts put into practice the ISE privacy guidelines defined in the *Privacy and Civil Liberties Policy Guidance Memorandum 2009-01* (June 2009).

To aid in its mission to protect critical infrastructure and key resources (CIKR), DHS established an information-sharing network called for in the *National Infrastructure Protection Plan v1* (2005). In April 2007, the ISE Program Manager designated the CIKR network as the private sector component of the ISE, and designated the DHS Assistant Secretary for Infrastructure Protection as the executive agent for integrating the CIKR information-sharing network and its private sector users into the ISE.

Federal Law Enforcement Information Sharing

The Department of Justice (DoJ) published its *Law Enforcement Information Sharing Plan* in October 2005. The DoJ plan "creates a forum for collaboration on how existing and planned systems will be coordinated and unified for information sharing

purposes." It also "establishes DoJ's commitment to move from a culture of 'need to know' toward a culture of 'need to share' in which information is shared as a matter of standard operating procedure." Its ultimate objective is to "help bring together the law enforcement community in the common cause of achieving multi-jurisdictional information sharing."

Under the Justice "information sharing" umbrella, the Global Justice Information Sharing Initiative is a federal government advisory committee that advises the U.S. Attorney General on initiatives for sharing and integration of justice and law-enforcement information. Within this initiative, there are five working groups (WGs) of Global Advisory Committee members and subject matter experts. The Global Security WG is developing or recommending best practices for "trusted" information sharing among legacy networks/systems across the Justice community. The major product of the Global Security WG to date has been its Applying Security Practices to Justice Information Sharing CD, intended to raise awareness and educate DoJ executives and managers on good fundamental security practices. The WG is also developing policy and guidance with regard to Global federated identity and privilege management, wireless security, and security architecture, as well as privacy policy.

The Global Privacy and Information Quality WG of privacy and local, state, tribal, and federal justice entity representatives are defining guidance on managing information quality, privacy, civil rights, and civil liberty risks; these risks could arise from or during sharing of Justice intelligence or biometric information, as well as assuring the quality of all shared Justice information, privacy and civil rights, and civil liberties of those to/about whom the information pertains.

The DoJ was designated executive agent in December 2009 of the *Nationwide Suspicious Activity Reporting Initiative (NSI)* called for in the *National Strategy for Information Sharing*. To implement the NSI, the DoJ is developing and implementing processes and policies for collecting, processing, and sharing information about suspicious terrorism-related activities. The NSI is also intended to ensure that information received and reviewed at any of the national information fusion centers will be quickly routed to and analyzed by the FBI's Joint Terrorism Task Forces to determine whether further investigation is warranted.

Multi-Agency Information Sharing Initiatives

The Defense Intelligence Information Enterprise (DI2E) is intended to integrate all disconnected DoD and IC information, teams, tools, and technologies into a single, all-encompassing system that will enable DoD and IC to more easily share information and resources. A memorandum of agreement was signed by the DoD and IC CIOs in June 2009, establishing a joint standards effort to define standards for DI2E.

The National Information Exchange Model (NIEM), established in December 2010, is defining a standard model for cross-domain information sharing across the federal government. Different members, alone or in partnership, are responsible for defining the information sharing formats for the different information domains supported by NIEM.

Specifically, NIEM is developing a range of standard XML schemas for translating data from disparate systems' various information formats into a single XML representation that can be understood by all XML-conversant applications. XML schemas are being defined for 12 domains of information. The last remaining domain, which is still being stood up, will result in an XML schema for sharing of cyber data (*e.g.,* schema for formatting data about cyberterror/cyberwarfare attacks and other cybersecurity incidents).

Future developments planned by NIEM include institutionalization of a common privacy and security framework for governance of information sharing, and the establishment of NIEM.ca to support cross-domain sharing with coalition partners. In addition, as the infrastructure domain agent for NIEM, DHS envisions providing a standard set of NIEM cross-domain support services. A DoD research and development initiative, the Cross-Domain Information Exchange Framework (CIEF) [2], was undertaken to enable NIEM's cross-domain information sharing services. The CIEF defines a universal XML-based framework for exchange of Global Information Grid (GIG) information that will provide an intelligent filter to ensure that all information exchanges in the GIG are correctly routed, at the correct times, and to the correct locations. In Fiscal Year 2010 eGov architecture guidance, the OMB identified NIEM as a federal best practice for cross-domain information sharing.

The Multi-Agency Collaboration Environment (MACE) is a pilot by interagency alliances of partners that will demonstrate information sharing within a common enterprise architecture. Specifically, the pilot is intended to demonstrate the value of interagency information sharing in disrupting the financial networks relied upon by individuals and organizations that threaten U.S. national security, economic interests, and allies. The MACE pilot's objectives include facilitating information discovery, planning, and execution of operations across departmental and agency boundaries.

The Federal Identity, Credential, and Access Management (FICAM) is a key enabler for responsible information sharing. In the face of disparate stove piped ICAM initiatives, the President, in 2004, signed *Homeland Security Presidential Directive-12* (HSPD-12), Policy for a Common Identification

Standard for Federal Employees and Contractors. HSPD-12 was designed in the hopes of achieving a single, fully horizontal (cross-organization) and fully vertical (cross-domain) FICAM framework for interoperability of ICAM systems and information across all federal government and government-supporting contractor collaborating/sharing participants, organizations, systems, and information stores in all security domains. In November 2009, the Identity, Credential, and Access Management Subcommittee (ICAMSC) within the FICAM Information Security and Identity Management Committee (ISIMC) released Part A of *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, which includes a FICAM segment architecture intended to drive the development and implementation of interoperable FICAM solutions.

The Universal Core (UCore) is an XML-based information exchange specification and implementation profile intended to facilitate information sharing by defining standard XML expressions of important concepts, including information sensitivity concepts, so that they can be uniformly expressed and universally understood in exchanges between different data-sharing communities. Version 1.0 of the UCore specification was published jointly by DoD and the IC in 2007. It included use of security metadata markings from the IC Controlled Access Program Coordination Office (CAPCO) Intelligence Community Information Security Markings (IC-ISM) 2.1 standard, with additional resource data tags to support ICAM. Data owners are expected to add other non-UCore security and community-specific data tags (*e.g.,* DoD Discovery Metadata Specification) to their data as appropriate. UCore was then expanded to address additional DoD and IC requirements, as well as requirements from DHS and DoJ. Future UCore enhancements are planned, including the addition of mechanisms and indicators for information provenance and confidence, and improvements in governance, policy, and oversight.

The Committee on National Security Systems published its *Frequently Asked Questions (FAQ) on Incidents and Spills* (CNSS-079-07) in August 2007 and its *National Instruction on Classified Information Spillage* (CNSS Instruction 1001) in February 2008. These provide information and guidance for all federal government classified system operators, especially those involved in cross-domain information sharing, on handling of and recovery from unintentional and intentional disclosure and loss of classified data beyond domain boundaries.

Multinational Initiatives

The Multilateral Interoperability Programme (MIP) is a North Atlantic Treaty Organization (NATO) initiative established to develop or improve interface specifications that will overcome the interoperability gaps between different NATO member Command and Control information systems enabling the multinational or coalition sharing of Command and Control information. MIP will implement the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) promulgated in NATO STANAG 55254.

The Trans-global Secure Collaborative Program (TSCP) is a multi-national public/private initiative that predates 9/11. Its mission is defining specifications for secure collaboration among participants in acquisition and supply chains. Such specifications include identity management, access control and privilege management, and information and resource management marking. Specifications defined by the TSCP include secure e-mail (implemented in CertiPath), document-sharing and identity federation, and digital rights management for intellectual property protection within product life cycle management environments. Additional specifications focus on export control within the same environments. [3,4,5]

Conclusion

All of these mandates and initiatives have transformed the information sharing culture in DoD and broader government. Prospective information consumers would formerly have had to demonstrate to the information owner their "need-to-know" of the information they wished to access, and even then, the decision of whether to share that information remained entirely with the information owner, who may still have withheld the information.

Information owners today are called on to fulfill a "responsibility to share." The "assurance" in *assured information sharing* was assurance that the information would be accessible to all prospective consumers who needed the information, as long as those consumers were determined to be sufficiently trustworthy to handle the information responsibly once it was in their custody. Information owners could no longer justify refusing to share information simply out of a desire to retain control over it. Before they could refuse to share, owners had to demonstrate that sharing certain information with certain prospective consumers under certain circumstances created an unacceptable risk of inappropriate disclosure, modification, or misappropriate use of the information by the prospective consumer. In other words, the owner had to demonstrate that the consumer was not sufficiently trustworthy to handle the information requested, and/or that the risks associated with sharing the information with that consumer outweighed the consumer's need for the information.

Such risks do exist, and after 10 years of a shift from miserly information sharing to information sharing profligacy, DoD and the broader government have recognized that a better balance needs to exist between

the information consumer's need for information, and the information owner's concerns over the risks that come with loss of control over the information. That balance is reflected by the fact that the imperative is no longer "assured information sharing," but is now "responsible information sharing."

The following quote articulates what part two of this series will address: "Sharing of information led to unauthorized disclosures on the Internet and in the media that have reportedly jeopardized intelligence sources and undermined U.S. diplomacy…The expanded use of computer networks has also increased the opportunity for even a single authorized user to access, copy, manipulate, download, and intentionally publicize enormous amounts of information from the interconnected databases of interconnected agencies." [6] ■

About the Author

Karen Mercedes Goertzel | is a Certified Information Systems Security Professional and leads Booz Allen's Information Security Research and Technology Intelligence Service. An expert in software assurance, information and communications technology (ICT) supply chain risk management, assured information sharing, and the insider threat to information systems, she has performed in-depth research and analysis for customers in the DoD, the IC, civilian agencies, NATO, and defense establishments in the U.K., Australia, and Canada. She was lead author/editor of Information Assurance Technology Analysis Center's (IATAC) State-of-the-Art Reports on Security Risk Management for the Off-the-Shelf ICT Supply Chain, The Insider Threat to Information Systems, and Software Security Assurance as well as a number of other IATAC information products and peer-reviewed journal articles and conference papers on these and other information assurance/cybersecurity topics. She can be contacted at *iatac@dtic.mil*.

References

1. For more information, see Bailey, Marianne, "The Unified Cross Domain Management Office: Bridging Security Domains and Cultures." In *CrossTalk: The Journal of Defense Software Engineering*, Volume 21 Issue 7, July 2008.
2. Shaw, Paul, and David J. Roberts, "The Cross-Domain Information Exchange Framework (CIEF)." Presented at AFCEA-GMU Critical Issues in C4I Symposium, Fairfax, VA, 20-21 May 2008.
3. Grant, Paul, and Jeff Nigriny, "Secure Information Sharing--Part I: Shaping Industry Interaction." In *Defense AT&L*, Volume 37, No. 1, January/February 2008.
4. Skedd, Richard, and Paul Grant, "Shaping Industry Interaction through Secure Information Sharing--Part II: Collaborating to Improve Collaboration." In *Defense AT&L*, Volume 37, No. 2, March/April 2008.
5. Grant, Paul, Jim Cisneros, and Jeff Nigriny, "Shaping Industry Interaction through Secure Information Sharing--Part III: Putting Theory into Practice." In *Defense AT&L*, Volume 37, No. 3, May/June 2008.
6. Takai, Teresa, Chief Information Officer and Acting Assistant Secretary of Defense for Networks and Information and Integration, and Thomas Ferguson, Principal Deputy Under Secretary of Defense for Intelligence, *Joint Statement for the Record*, presented to the U.S. Congress, Senate, Committee on Homeland Security and Governmental Affairs Hearing on "Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration," 21 March 2011.

Not Just the U.S.

Since 9/11, other countries have undertaken numerous information sharing initiatives:

- **European Union**: Information Sharing and Analysis Center (ISAC) Foundation; National and European Information Sharing and Alerting System (NEISAS)
- **NATO**: Transformation Network (TRANSNET); NATO Research and Technology Organisation Trusted Information Sharing for Partnerships
- **Interpol**: I-Link
- **Organisation for Economic Co-operation and Development (OECD)**: Agreement on Exchange of Information on Tax Matters
- **International Standards Organization/International Electrotechnical Committee**: ISO/IEC 27010, Information security management for inter-sector and inter-organisational communications
- **Asia**: Economic Information Sharing Mechanism of the Asia-Pacific (EiSMAP); Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) Information Sharing Centre
- **New Zealand**: Parliament's proposed Privacy (Information Sharing) Bill
- **Germany**: Information Sharing National Strategy
- **Australia**: National Government Information Sharing Strategy; Trusted Information Sharing Network
- **Canada**: Information Sharing and Analysis Centres
- **Russia**: Federal Customs Service M-Exchange.

There are also numerous U.S. private sector initiatives that have grown out of post-9/11 government information sharing mandates including, notably, the private-sector Information Sharing and Analysis Centers (ISACs).

IEEE Symposium on Security and Privacy

The Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy will take place on May 20-23, 2012 in San Francisco, CA. This event targets researchers and practitioners, and focuses on computer security and electronic privacy advancements. The IEEE Symposium will focus on the following topics: Web 2.0 Security and Privacy, Mobile Security Technologies, Research for Insider Threat, Semantic Computing and Security, and Trustworthy Embedded Systems.

The conference will have 12 information assurance-related sessions including Malware, Attacks, Access Control and Attestation, Privacy and Anonymity, and others. Presenters from Carnegie Mellon University, University of Texas at Austin, Cornell, as well as several international universities—University of Cambridge, ETH Zurich, and Peking University—will deliver papers on relevant topics.

IEEE Security and Privacy Workshops will be co-located with the symposium. Workshops will offer participants the opportunity to delve deeper into specific aspects of security and privacy. For more information about this event or other IEEE events, please visit *http://ieee.org*. [1] ■

References

1. *http://www.ieee-security.org/TC/SP2012/index.html*

DoD IA Symposium

28–30 August 2012 | Nashville, TN

The Department of Defense (DoD) Information Assurance Symposium (IAS) will take place 28-30 August 2012 at the Gaylord Opryland Resort and Convention Center in Nashville, TN. It will bring together leaders and IA practitioners from across government, industry, and academia to network and explore ways to improve IA.

- To attend, contact ***www.iad.gov/events*** for more information.
- To participate in the IA Exposition, which will take place in conjunction with IAS, visit ***www.informationassuranceexpo.com/.***

The Open Web Application Security Project: Secure Web Code Development

by Kevin McLaughlin and Konstantin Ivanov

This article provides an overview of the Open Web Application Security Project (OWASP) organization and its methodology. This article discusses the benefits that OWASP brings to an organization and a personal approach to implementing OWASP standards in an information technology (IT) environment that currently does not use them. The benefits to an organization include the various reasons as to why the OWASP approach benefits not only an IT group, but the organization as a whole. Finally, this article details the implementation of this system in a hypothetical scenario.

Introduction to OWASP

In an increasingly interconnected world that is driven by constant technological evolution, software and Web applications are capable of doing more than ever before. Users are empowered with tools that allow them to chat with other users halfway across the world, and to even control their finances completely online. Today's user empowerment, unfortunately, opens the door for malicious activity. Malicious online activity that exploits the vulnerabilities in commercial or customized Web applications has created a niche for OWASP to fill. OWASP was originally founded in December 2001, and was later established as a not-for-profit charitable organization in 2004. "OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted." [1]

OWASP provides tools, downloads, references, *etc.* that are free and open to the public with the end goal of developing and providing additional material to help software developers create safer and more secure applications. As stated on their Web site, many of the OWASP projects are open source and collaborative with high levels of developer and community input, with the hope that it will ultimately result in more secure code coming from the participants, and that the use of the OWASP secure coding methodologies and practices will catch on across the worldwide developer community.

Video OWASP Application Security (Appsec) Tutorial Series (Source: *http://www.youtube.com/watch?v=CDbWvEwBBxo&feature=results_video&playnext=1&list=PL8239DA448CC2BB7C*)

One of the primary OWASP foundation management core values is Open, meaning that everything is radically transparent, from finances to code. [2] The other three management values adopted by the OWASP foundation are Innovation, Global, and Integrity. The OWASP foundation Web site materials are definitely geared towards the tech heavy software coding crowd; although, at a high level, it is easy for non-programmer techies to understand the purpose of the materials. The OWASP materials tend to operate on a code-based level because that is where the damage of vulnerabilities and exploits really occur. One distinction that needs to be made is that OWASP's primary focus and mission is on Web application software and how to make that type of software more secure. The OWASP focus is on building secure Web software, not on securing the associated hardware components.

A core OWASP tenet is explained in a video by OWASP, "Defensive Coding," which is the term that Web software developers should keep in mind when they are building or securing an application. The concept of defensive coding, in theory, will inherently raise the speed of growth versus the need to secure the application debate that has to

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross-Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
Was T10 2004 A10 – Insecure Configuration Management	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cyrptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
Not in T10 2007	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	*Dropped from T10 2010*
A6 – Information Leakage and Improper Error Handling	*Dropped from T10 2010*

Table 1 2010 top 10 most dangerous vulnerabilities

take place for Web programmers to meet both the business need for the application and the organization's compliance need for the application to be compliant with all the regulatory compliance areas to which the organization is mandated to adhere.

Table 1 displays an OWASP graph with the top 10 most dangerous vulnerabilities of 2010 and how they historically compare to the previous top 10 most dangerous vulnerabilities. [3] The OWASP foundation updates this list annually.

It is interesting to note that even after all these years of hearing about injection attacks, it still tops the list of vulnerabilities. In a report published by Hewlett-Packard (HP), they noted that in a survey they conducted on 236 static Web applications, 69% contained Structured Query Language (SQL) injection vulnerabilities and 42% contained XSS vulnerabilities. HP has also mentioned that there were over 30,000,000 Web application attacks last year, and that record has already been broken in the first half of this year alone. More concerning is that in other reports, there were upwards of 3,000 application vulnerabilities disclosed in the first half of 2011. [4] SQL injections and XSS remain the overwhelming popular choices in breaching Web sites and Web applications. Vulnerabilities often occur due to poor coding or SQL queries with little thought to long-term code management, structure, best-practice use, apathy, and an overall lack of knowledge on the part of some developers, which leads to these relatively simple-to-fix coding security flaws.

As most security professionals can tell you, an item that adds additional concern to the issue of unsecure code implementation is the almost knee-jerk "false positive" reaction by Web developers whenever security professionals or application vulnerability scanning software discovers a vulnerability in their code. While we spend time arguing about whether an item is a false positive or not, we continue to experience application breaches that result in stolen data,

financial damage, and both tangible and intangible losses to private, public, and government business entities. Statistics, like the ones touted in the HP survey and the one by Dausin in 2011, enforce the need for organizations, such as the OWASP foundation, to help combat these issues and increase the security knowledge across the worldwide developer community.

Benefits to an Organization

Organizations would benefit by having a reduced amount of Web code exploitable vulnerabilities if they started to require their Web application developers to follow the secure coding guidelines and best practices advocated by the OWASP foundation. OWASP items are a best-practice, up-to-date, and verified approach to better develop safe and secure applications and protect the organizational data that the information and communications technology (ICT) and information security/assurance professional's working for an organization are entrusted to safeguard.

In case studies done to not only apply but to test the validity of OWASP's methods, the results indicate that following OWASP methodologies contributed significantly in developing better secured Web applications. At a minimum, there was a significant reduction in the number of exploitable security vulnerabilities in Web-based university applications that were written using OWASP methodologies. [5] Although not yet conclusive, studies have shown the validity and effectiveness of OWASP's methods and their ability to better secure organizational data.

From personal experience in an Oracle Service Business development environment, we can say that without proper planning and best practices, coding quickly becomes a nightmare as every employee has their own technique. The issues surrounding the specific and often unique coding technique that each developer uses really becomes compounded when a coder leaves the company as the remaining developers must then decipher the work left behind. This, unfortunately, is a regular occurrence in many IT groups. The quick evolution of technologies and constant movement of IT professionals makes it difficult to implement application standards in many environments or to even provide basic continuity. This movement is just one of the many problems and concerns that the OWASP framework discusses and addresses.

From a managerial perspective, OWASP brings tested crowd-sourced methodologies and a sense of order to Web application code. In many organizations, there is still a great emphasis from a management perspective on metrics and measurable accomplishments. There will always be a challenge in ICT with providing a firm metric or statistic on how secure an application truly is; luckily, this is part of the OWASP framework. Using the RiskDread analysis, an application can be tested and rated in a structured way. The equation used for this is *RiskDread = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability)/5.* [6] This formula rates an application's security on a scale of 0 to 10 with 10 being the highest risk application. After running applications through this formula, the numbers can then be presented to management as a firm measurement of application risk using an easy-to-present overview of the highest to lowest risk applications.

Since many managers are concerned with financial constraints, one very clear business advantage is that OWASP is free and open-sourced, which helps keep training, hardware infrastructure, software purchases, consulting fees, *etc.* to a minimum. If a company decides that additional OWASP help is needed to kick-start their OWASP, OWASP is available to consult on a per hour basis. [7] OWASP not only provides the metrics and formalized best practices that managers like to see, it also provides a cost effective alternative to paying for additional resources.

From a coding perspective, OWASP provides terrific code examples and structures on a technologically agnostic approach. The tools and methodologies provided by OWASP are hardware and software neutral, allowing virtually all application coders to apply the methods. The OWASP foundation also provides sample projects, sample code, discussion/communication forums, code reviews, best-practice PDFs, and wikis and how-to's on virtually every aspect of securing Web applications. The OWASP list of resources is exhaustive and ever growing.

Threat Modeling Process
1. Identify Assets
2. Create an Architecture Overview
3. Decompose the Application
4. Identify the Threats
5. Document the Threats
6. Rate the Threats

Table 2 Threat modeling process

Alluding to an earlier point about managing chaos and organization change, a strong argument can be made that if strong methodology is implemented within a coding group, standardization and development is then much easier, making the code much more secure. This rigor provides a structured, logical, and technologically proven path to building and maintaining secure Web applications with a defensive coding mentality.

To assist in managerial reporting needs, OWASP also includes a multiple threat management modeling process like that depicted in Table 2. [8]

Personal Adoption of OWASP

A good process to use as an ICT development team manager building the adoption of effective OWASP standards

into the organizational application development methodology is to slowly introduce the OWASP concept and framework to the organization's application development team. Just as Rome was not built in a day, coding and application standards are not going to be built and adopted in a day. Without going off on a tangent about ICT adoption theory, keep in mind that change is difficult for employees to accept [9,10]; it might be harder than normal for your team of developers to accept these new standards. ICT development team managers should take a very methodical and logical approach into not just rolling out the technical materials that come with OWASP, but a mentality change in how things should be done. The two biggest hurdles that we envision are the technological change and the employee buy-in of the mentality change. ICT development team managers must first work on switching the application developer's mentality from where it is currently to one of constantly thinking about defensive coding. These managers need to push the concepts of best practices and standards to their developers, and establish a training program that does so in a way that the OWASP methodologies are soon established as a core and integral part of writing Web applications for the organization.

Once the development team members buy into the defensive coding mentality, then work has to take place to change the associated technical processes. Since OWASP is technologically neutral, the IT tools and coding languages (*e.g.,* Java, .Net, PHP) would remain the same; however, how the Web applications are coded and secured would change. The actual code, documentation, risk analysis and reporting, and overall work processes might also experience some change.

Conclusion

Technological growth is an enabler for both regular users and the Black Hat community alike. Unfortunately, Web applications are not immune to cyber crime and exploits; they actually seem to be a much targeted attack vector. To combat this, organizations need to implement proven secure methodologies such as the one that OWASP offers. The adoption of these types of best practice methodologies may greatly reduce the risk of suffering from Web application hacks and breaches that are targeting relatively easy-to-remediate software coding vulnerabilities. Breaches caused by inadequately secured software and poorly written Web application code can cause large dollar amounts of tangible and intangible losses to an organization. Using methodologies like the OWASP defensive coding, one may not completely eradicate the risk, but it will greatly reduce it. OWASP provides a way to better protect Web applications at a very cost effective rate to the organization. ■

About the Authors

Kevin L. McLaughlin | began his career as a Special Agent for the Department of Army. He was responsible for investigating felony crimes around the globe. He was a Director at the Kennedy Space Center, the President of his own company, and an IT Manager and Senior Information Security manager with the Procter & Gamble (P&G) company. While at P&G, he created one of their augmentation outsourcing teams in India, which won a global Gold Service award from Atos-Origin that has acted as a model for countless corporate relationships since. Mr. McLaughlin joined the University of Cincinnati in April 2006 to create an Information Security program and build a team of information security professionals. He is responsible for all aspects of information security management, including but not limited to strategic planning and the architecture and design of information security solutions. Mr. McLaughlin is currently an Information Security/Assurance Doctorial candidate with the University of Fairfax. He has his M.S. in Computer Science Education and his B.S in Management of Information Systems. Mr. McLaughlin has the following certifications: Certified Information Security Manager, Certified Information Systems Security Professional, Project Management Professional, ITIL Master Certified, Global Information Assurance Certification Security Leadership Certificate, and Certified in Risk and Information Systems Control. He can be contacted at *iatac@dtic.mil.*

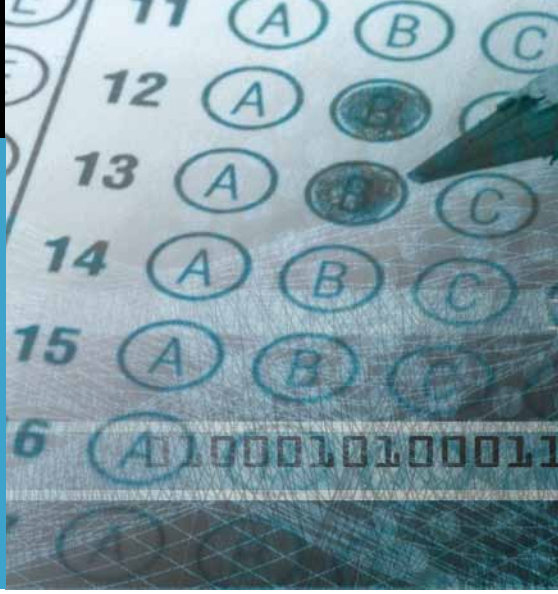
Konstantin Ivanov | is a recent graduate of the University of Cincinnati with a B.S. in Information Systems, and is actively pursuing his M.S. As a Global Data Services Analyst with Chiquita Brands, Mr. Ivanov's primary focus is in database administration, development, and project management. He has interned with General Electric as well as with Chiquita Brands, and has also worked as an IT consultant with Faculty Technology Resources Center at the University of Cincinnati during his undergraduate program. He can be contacted at *iatac@dtic.mil.*

References

1. OWASP, F. About the open Web application security project - OWASP. 2011 [cited 2011 September 24]. *https://www.owasp.org/index.php/About_OWASP.*
2. *Ibid.*
3. *Ibid.*
4. Dausin, M., The 2011 mid-year top cyber security risks report. Hewlett Packard, 2011. HP DVLabs.
5. Sedek, K., Developing a secure web application using OWASP guidelines. CCSE - Computer and Information Science, 2009. November 2009.
6. *Ibid.*
7. Consultant. Consulting fee rates. 2006 [cited 2011 14 October]; Available from: *http://www.consultantjournal.com/blog/setting-consulting-fee-rates.*
8. Microsoft. Threat model your security risks. MSDN Magazine 2003 [cited 2011 14 October]. *http://msdn.microsoft.com/en-us/magazine/cc164068.aspx.*
9. Larkin, B., Increasing information integrity:Cultural impacts of changing the way we manage data International Journal of Organization Theory and Behavior, 2008. 11(4): p. 558.
10. Blanchard, K., Mastering the art of change: Ken Blanchard offers some strategies for successfully leading change. Training Journal, 2010: p. 44.

Certification Spotlight: Offensive Security's OSCP

by Chris Merritt



Editor's Note: The following article presents an author's perspective that is in no way endorsed by the Department of Defense, the Information Assurance Technology Analysis Center, or the *IAnewsletter*.

Many certifying bodies use multiple choice tests to assess knowledge and substantiate proficiency in a certain professional discipline either by choice or because the expertise in the subject matter cannot easily be demonstrated (vice tested) by potential candidates. For example, it would be tough for the Project Management Institute™ to derive a mechanism to demonstrate proficiency for project management professionals in any manner other than a written test. The alternative might be to give candidates a project to manage, monitor their approach, evaluate the success of the project, and only then provide their Project Management Professional (PMP) credential, but this is not really reasonable or feasible. In the world of penetration testing, however, this is exactly the approach one certification follows.

In this article, we examine the Offensive Security Certified Professional (OSCP) certification as a case study into improving information technology (IT) certifications. It requires candidates to demonstrate proficiency in a lab rather than simply memorizing facts and reciting them on a written test.

The OSCP credential substantiates real-world skill sets by requiring candidates to immerse themselves into a diverse environment where they ultimately exploit weaknesses within the environment.

Recently, there has been a lot of discussion on the true value of professional certifications, including their short comings and overall benefit to various professional industries. [1] The model used by Offensive Security to provide this certification in penetration testing helps substantiate an individual's ability to apply his or her expertise in real-world settings for IA professional communities.

Mr. Mati Aharoni, Founder and Lead Trainer for Offensive Security's penetration testing certification, wrote, "What we are testing is two-fold. First, the technical skills that you have obtained in the course of training. Second, we are testing your ability to think out of the box in a real-world situation. Some of the systems the students encounter in the course of the exam are not covered directly in the course of training; however, by using the skills that are covered in the training, they should be able to solve the problems. While some may consider this to be unfair, we believe this is extremely important to ensure that all certified personnel have proven they do far more than simply memorize…information."

This approach sets Offensive Security's certification apart from other similar certifications. The OSCP credential substantiates real-world skill sets by requiring candidates to immerse themselves into a diverse environment, where they are expected to craft custom exploits, seek out and identify security flaws, and ultimately exploit weaknesses within the environment to successfully navigate the certification process. The *Penetration Testing with BackTrack* course—the training for the OSCP certification—simulates a full penetration test from beginning to end, and provides each student with knowledge about necessary tools and testing/exploiting approaches required to compromise targets during the certification challenge.

Though OSCP does not disclose the pass/fail rates, there is evidence that the

practical exam is challenging. Mr. Aharoni says, "We do experience that students are required to put significantly more effort than what they may be used to from other certification scenarios. Those that don't put out the effort often find they have to re-take the exam."

Mr. Aharoni states that the ideal candidate for the OSCP certification "is someone that has a strong technical background that has experience in both Windows and Linux, with a solid understanding of network administration. Additionally, our courses require a strong commitment and the sort of personality that is determined and motivated to obtain a solid understanding of information security issues. It is worth mentioning that the current *Penetration Testing with Backtrack* course was originally named *Offensive Security 101* as we felt it represented the foundational level of understanding that is required in the industry; however, we found that students that had previously attended other training programs were unprepared for the level of effort that our course required. In the end, we had to change the name to *Penetration Testing with Backtrack* in order to better set expectations."

It appears that the OSCP penetration testing certification has provided practitioners with a higher degree of proficiency. The Chief Technology Officer and Lead Security Researcher at Proso, Nick Popovich, has positive things to say about his experience traversing the OSCP training and certification process. He notes that this particular certification is truly a difference-maker when it comes to pursuing penetration testing work in both the private and public sectors.

Offensive Security has offered the OSCP certification since 2006, and it has gained traction in the information security and penetration testing segments of the IT business. This may be attributed to the value it brings to organizations that do in-house penetration testing or provide penetration testing services. It is also important to note that Offensive Security "has students from various backgrounds outside of security that gain a lot from the courses. For instance, system administrators find that the understanding they gain in the course of the *Penetration Testing With BackTrack* gives them a deeper understanding of not just how to better secure their systems from attack, but also stretches them and helps them be better system administrators overall. This is true as well for our *Advanced Windows Exploitation* course, as Windows programmers find they gain a better understanding on the sorts of common mistakes that are made in programs that allow exploitation to occur."

The Offensive Security approach is one that warrants a closer look. It is a shame that all certifications across all disciplines cannot be provided based upon performance and real-world demonstration of mastery in a particular area. Because of the nature of many disciplines, this approach to certification is simply not an option, so multiple choice will likely continue. Where credentials *can* be validated by demonstration, multiple choice tests should not be used. The preferred method for credentials that *can* be confirmed by real-world application should be. ■

About the Author

Chris Merritt | is founder of Prolific Solutions, a security consulting and software company, and has recently launched MyCPEs.com [2], a free Web site that helps certified professionals across all industries manage and maintain their professional certifications and continuing education requirements. He can be contacted at *iatac@dtic.mil*.

References

1. *http://mycpes.com/blog/post/2011/11/04/Are-Certifications-a-Money-Driven-Racket.aspx*
2. *https://www.mycpes.com/blog/post/2011/11/25/Certification-Spotlight-Offensive-Security-OSCP.aspx?AspxAutoDetectCookieSupport=1*

IATAC Connects Using Social Media

by Jarad Kopf and David Lee

The Information Assurance Technology Analysis Center (IATAC) has been leveraging social media to actively reach out to the information assurance (IA) and cybersecurity communities across government, industry, and academia. This article profiles IATAC's efforts across two major social media platforms: Twitter and LinkedIn.

IA professionals looking for answers to their most difficult IA and cybersecurity questions can use LinkedIn to access IATAC's free research services.

Twitter

With over 100 million users and counting, Twitter has one of the fastest growing user bases. IATAC has leveraged Twitter for multiple facets of spreading the word on IA and cybersecurity. The IATAC Twitter feed (*@DTIC_IATAC*) serves as an area where our products are put on display and advertised for greater visibility to the public.

In addition to advertising products, we retweet and highlight our favorite articles that mention our products and services.

@DTIC_IATAC has received multiple IA-related questions about cyber, information security, and other relevant IA topics. IATAC has provided these Twitter followers with 4 hours of free IA research through its Technical Inquiries program, a free research service that IATAC offers to its customers.

In addition, @DTIC_IATAC is one of the best ways to stay up to date on current IA articles from around the Internet.

IATAC encourages you to follow us and retweet our articles to your friends and colleagues. With our growing membership, @DTIC_IATAC is quickly growing into a source of information for all of your IA and cybersecurity needs… in 140 characters or less!

LinkedIn

IATAC has also been utilizing the social media network, LinkedIn, to connect globally with like-minded IA and information technology professionals. Since LinkedIn is a publicly available social media network focused on linking professional colleagues, IATAC recognizes its value in helping IA

Video How to join and search for groups on LinkedIn
(Source: *http://www.youtube.com/watch?v=4OyZdeW5GAo*)

professionals connect across all sectors—government, industry, and academia. Through LinkedIn, IATAC has been able to generate a forum in which IA and cybersecurity ideas, current events, and questions can be shared and discussed.

IA professionals looking for answers to their most difficult IA and cybersecurity questions can use LinkedIn to access IATAC's free research services. Members frequently post current news articles for the forum group, which spark discussions on a variety of cybersecurity topics. Along with the online discussions, members also share opinions, which lead to healthy debates.

IATAC also leverages LinkedIn to promote its free products and services, such as the *IANewsletter*, State-of-the-Art Reports, and Tools Reports. The IATAC LinkedIn group currently has reached over 440 members with a vast array of job titles spanning many different countries. The group is continuously growing with more people joining every day.

To join the group, go to *http://www.linkedin.com/groups?gid=2191589&trk=group-name* or search for the group name "IATAC" on LinkedIn. IATAC looks forward to collaborating with you on LinkedIn in the future!

Conclusion

IATAC is excited to be able to share information and collaborate more freely with its long-standing customers—and to reach new customers—through these publicly available social media platforms. Both Twitter and LinkedIn serve as valuable resources for sharing information about IATAC's resources and current IA and cybersecurity events. More importantly, however, they enable IATAC to better connect with the professional communities we serve and to understand their needs in real time. We hope you will connect with the IATAC LinkedIn group or follow IATAC on Twitter! ■

IATAC is excited to be able to share information and collaborate more freely with its long-standing customers—and to reach new customers—through these publicly available social media platforms.

About the Authors

Jarad Kopf | is a Scientific and Technical Information Deliverables Analyst for IATAC. Mr. Kopf has a Security+ Certification, an M.S. in Environmental Science from Christopher Newport University, and is currently pursuing a second M.S in Cybersecurity from University of Maryland University College. He can be contacted at *iatac@dtic.mil*.

David Lee | is a Senior Consultant at Booz Allen Hamilton. He is a Certified Information Privacy Professional. Mr. Lee has worked with the government with over 8 years of experience in the areas of the Freedom of Information Act, Records Management, and Privacy. He formerly served in the U.S. Navy aboard the USS SEATTLE and at the National Naval Medical Center as the lead paralegal for the Staff Judge Advocate's Office. He can be contacted at *iatac@dtic.mil*.

Business Continuity Planning, Disaster Recovery, and Government Regulation?

by Kevin L. McLaughlin

In light of recent natural disasters and the struggle that many businesses have with recovering from such an event, this question should be asked: should the government make business continuity/disaster recovery (DR) planning mandatory, or should that degree of control be up to the parties involved, with the courts deciding whether or not their choices were appropriate? Understanding the true costs of peer planning overall, and viewing these costs from an information assurance (IA) and information technology (IT) perspective adds a new dimension to this question.

Organizations continue to take large-scale losses and even go out of business by not adequately planning for large-scale disasters that impact their ability to conduct business. When a disaster hits an area, the socioeconomic impact it causes is compounded when the citizens of that area also end up out of work, displaced from their homes, and not receiving a pay check. The frustration caused by being out of work and delays in the deployment of acceptable, quality temporary housing lead many of the affected citizens to file civil lawsuits for damages. [1] These lawsuits frequently cite management neglect and lack of DR planning as one of the reasons for seeking damages, adding to the post-disaster economic distress suffered by communities and businesses. The negative effects of a disaster can damage communities and their citizens for a long time after the event. Although many items contribute to this slow recovery, "none are as debilitating as the litigation processes that…ensue to redress" the negative socioeconomic impact experienced by the members of the community. [2]

Background

Many organizations voluntarily spend money and time attempting to design systems, processes, and methodologies that will enable them to continue business operations in the event of a disaster. In light of disasters, like the March 2011 earthquake and tsunami in Japan, the Fukishima Daiichi nuclear power plant, and the April 2011 tornados that devastated parts of Alabama [3], it is important that organizations are able to contact the resources needed and that they have methods in place to ensure that resources can actually make it to the recovery area. Adding strong leadership roles for the responding resources is also of critical importance for successful post-event DR. [4]

Standards and Best Practices

There is currently a dearth of government regulation that requires business entities to have robust business continuity and DR plans, strategies, and infrastructure in place. There are, however, many standards in place that assist organizations in designing effective DR plans. The National Institute of Standards in Technology (NIST) Special Publication (SP) 800-34 is one such standard, and its book on contingency planning outlines methodologies for organizations to follow and strongly suggest that each organization have such plans in place so that they do not suffer unrecoverable post-disaster loss. NIST SP 800-34 recommends that organizations follow the seven steps depicted in Figure 1 in the event of a disaster. [5]

Figure 1 NIST SP 800-34 contingency planning process

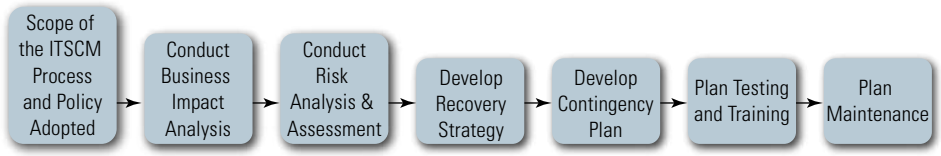


Figure 2 ITIL ITSCM process

The IT Information Library (ITIL) section on IT Service Continuity Management (ITSCM) is another publication that outlines contingency planning methodologies and infrastructure that businesses should be using for post DR. The ITIL ITSCM standard recommends the seven steps depicted in Figure 2. [6] Compare the two figures, and you can see that both of these standards-based approaches to business continuity and DR planning require the development of a policy, the completion of a business impact analysis, the development of a contingency plan, testing and training on the contingency plan, and ongoing plan maintenance.

Learnings from Natural Disasters

We have learned that recovering damaged infrastructure to their pre-disaster conditions can take years and is an expensive process—the reconstruction efforts for post-Katrina have cost in excess of $81B—that negatively impacts the economy of the affected area(s). [7] The psychological impacts of a disaster can also undermine the long-term mental health of the affected populace. [8] Tulane University thought it was prepared for an event like Katrina, but it did not have plans on how to recover from such an event and ended up missing its August payroll run, which compounded the trauma that many families were already going through. [9]

The aftermath of the Katrina disaster was tough on the communities impacted; better business continuity and DR planning would have gone a long ways towards minimizing the socioeconomic downfall that affected New Orleans and its surrounding communities. It took so long for universities in Louisiana and Mississippi to recover from the aftermath of Katrina that 26,000 students in Louisiana and 9,000 students in Mississippi failed to return to their schools. [10] Two years after the event, the University of New Orleans was still 6,000 students under its pre-Katrina enrollment numbers and Loyola University was still 1,000 students under its pre-Katrina enrollment numbers. A secondary impact of this drop in enrollment is that 217 faculty members who lived and worked in the New Orleans community were fired from their university positions. [11] These post-disaster numbers just within location institutions of higher education, the community of New Orleans had 7,217 less consumers spending money and helping their community rebuild and recover its economy.

Dollars and Sense

One of the major issues faced by organizations when they are considering DR strategies, such as integrated automation to facilitate DR high availability [12], is the large amount of budget money necessary to implement a successful business continuity and DR program. This budget is often needed on an annual basis, spent on contingency items, but might never be used. It is very difficult for managers within an organization to spend scarce dollars for an event that might never occur.

Senior managers for organizations need to understand that the infusion of technology across their business processes makes ignoring DR planning borderline gross neglect. [13] In many cases, the failure to follow all of the seven NIST SP 800-34 contingency planning steps to prepare for a disaster can be seen as a failure of the organization's senior management and lead to civil lawsuits for damages. This lack of prudence by organizational management can compound events to such an extent that the organization is incapable of post-event recovery. In some post-event cases, we can even go as far as to say that "managerial errors are the root causes of the lack of technological recovery after a disaster." [14]

Government Regulation

Government regulation of any process is a dual-edged sword that needs to be closely viewed along both of its edges. It is very easy to say that requiring business entities to have robust DR

infrastructure is the best way to ensure longevity, however, this is just too simple of an answer.

Taking a deeper look at whether government regulation is the catalyst that produces the behavioral changes necessary, we need to consider some of the historical results government regulation has produced. Bergland and Pederson, 1997, found that costly regulation induced "the individual rational fisherman to behave in a way which increases their risks" of injury. [15] This behavior is caused by a fundamental risk analysis being conducted on the part of the regulated entity.

Will it cost more to follow the regulation than it will to suffer the accident or loss caused by a negative event?

This is an impactful question that needs to be fully considered. [16] "Give me the right to go broke" is an often heard lament between industry and government when the topic of government regulation is brought up. [17] In 1982, U.S. Executive Order 12291 stated that "regulatory action shall not be undertaken unless the benefits to society…outweigh the costs to society." [18] This type of cost benefit analysis and risk versus cost-based thinking is a critical component to consider when deciding if DR management should be regulated by a government agency.

Some industry experts feel strongly that government regulation in the area of post-disaster Internet recovery operations would impede the self-regulatory steps many private companies are already taking in this area. [19] We can take a look at the apparent lack of impact that Federal Trade Commission regulations are having on Internet scams and e-mail phishing schemes, or that the Health Insurance Portability and Accountability Act (HIPAA) is having on non-disclosure of private medical information to help decide if government regulation is the solution that will drive organizations towards having robust DR plans, methodologies, and infrastructures put in place. In parallel with any regulatory effort, the government is also going to have to pay for an enforcement arm that will be responsible for monitoring and ensuring organizational compliance with the business continuity and DR regulations.

Laissez-Faire

There are also many proponents of leaving things as they are and allowing organizations and communities to self-regulate themselves. While the appeal of self-regulation is strong, all we have to do is take a look at the abject failure we have experienced at "protecting information privacy through industry self-regulation." [20] One of the motivations for the enactment of government regulation to an area is the perceived failure of the group or industry to self-regulate. The HIPAA regulations were created to fix the perceived failure of medical professionals to safeguard the confidentiality of the personal medical information of their patients. The Sarbanes-Oxley regulations were created to fix the perceived failure of public organizations (*e.g.,* Enron) to protect the integrity and authenticity of their financial records. Conversely, the Payment Card Industry requirements, which were created to fix the perceived failure of organizations involved in credit card transactions to safeguard and protect consumers credit card data, is an example of an area in which the private credit card companies provided self-regulation.

Conclusion

Government regulation can play an effective part in driving U.S.-based businesses towards putting basic DR plans and infrastructure in place. Such regulation would be appropriate as long as businesses are implementing them to minimize the post-disaster economic and psychological impact, and they were paying them attention to keep the regulatory cost down during the reconstruction period; however, "government regulations can be both golden rules to security's bottom line and a regular headache." [21] Organizations need to understand that if government regulations have to be put in place because of the doubt as to whether most businesses have adequate plans in place to successfully recover from a disastrous event, they may very well soon be forced into doing things that they do not want to do. Overall, even though the U.S. government has been quiet in regards to leveraging Internet, core IT, business continuity, and DR regulations onto businesses within the U.S., they tend to take the approach of allowing organizations to self-regulate much of their IT environment and processes. [22]

Lawsuits are also not the answer to resolving the issue of successful post-DR, and are actually counterproductive to the goal of maintaining a stable socioeconomic climate that is ripe for successful DR. [23] Many businesses who suffer a disaster do not have the financial means to recover and continue their operations in the community; having to pay post-disaster settlement costs will drive these businesses closer towards bankruptcy.

As the Chief Information Officer of an organization has a fiduciary responsibility to protect corporate assets in good times and bad, self-regulation is the other component they have to put in place if community businesses are to remain open and viable after a disaster strikes their geographical region. [24] Many businesses are already exploring DR infrastructure solutions of their own accord. "Data recovery is now a $20 billion-per-year sector of IT" [25], which is a strong indicator that the increasing number of recent natural and man-made disasters that have hit communities is causing organizations to start implementing DR plans and tools on their own. Organizations are starting to understand that developing and maintaining a comprehensive DR plan

and infrastructure is of critical importance. [26] The Loews Corporation, a New York-based holding company, in part because of the 9/11 disaster, has developed multiple points of redundancy and DR plans just in case they are impacted by future events. [27] Similarly, the ninth item on the list of the top 10 trends in higher education is to increase focus on planning for DR. [28] "I think the worst thing the government could do is not listen to the industry participants about what they are capable of doing." [29]

There are, however, many areas that the government can be involved in when it comes to protecting the U.S. infrastructure and improving DR among government and private organizations. One area is to assist in the development of standards, best practices, and training. [30] Good examples of the type of standards and best practices that governments can develop and promote are the U.S. Government NIST 800-34 contingency planning and the U.K. Government ITIL continuity planning. Another area is in the training of post-event reconstruction methodologies that cover how the initial series of reconstruction decisions need to be made quickly and correctly: "Despite the urgency with which these decisions are made, they have long-term impacts, changing the lives of those affected by the disaster for years to come." [31] As these decisions are extremely impactful to the affected populace, it is critical that adequate training be provided to the policy makers that make them.

A combination of government regulation, self-regulation, government, and private training of business continuity/DR professionals and government and private sector partnerships and associations is necessary to minimize the negative socioeconomic impact caused by a large-scale disaster. The partnership programs should be modeled after the Federal Emergency Management Agency's free post 9/11 integrated government and private sector training for emergency responders across the U.S. [32] The business continuity/DR integrated training courses should consist of free nationwide awareness classes on why businesses need to worry about and prepare for a disaster that impacts their ability to conduct business and the economic impact suffered by their community when they fail to go back in business post disaster. Additional courses should be offered to business and IT management on the seven NIST 800-34 contingency and ITIL continuity planning steps, as well as the guidelines for effective post-event reconstruction. ■

About the Author

Kevin L. McLaughlin | See bio on page 23.

References

1. El-Anwar, O., K. el-Rayes, and A. Elnashai, Minimization of socioeconomic disruption for displaced populations following disasters. Disasters, 2010. 34(3): p. 865-883.
2. Picou, J.S., B.K. Marshall, and D.A. Gill, Disaster, litigation and the corrosive community. The University of North Carolina Press: Social Forces, 2004. 82(4): p. 1493-1522.
3. Wagman, D., When Disasters Strike. Power Engineering, 2011. 115(6): p. 4-4.
4. Biddinger, N., The information technology role in disaster recovery and business continuity. Government Finance Review, 2007. 23(6): p. 54-56.
5. Swanson, M., *et al.,* National Institute of Standards and Technology 800-34. Contingency planning guide for information technology systems, 2002: p. 1-H1.
6. The official introduction to the ITIL service lifecycle. 2007, London, United Kingdom: Office of Government Commerce on behalf of the Crown.
7. Orabi, W., Senouci, Ahmed B., K. El-Rayes, and H. Al-Derham, Optimizing Resource Utilization during the Recovery of Civil Infrastructure Systems. Journal of Management in Engineering, 2010. 26(4): p. 237-246.
8. Bava, S., *et al.,* Lessons in Collaboration, Four Years Post-Katrina. Family Process, 2010. 49: p. 543-558.
9. Anthes, G., Tulane University; Following Katrina, the university's top priority was getting its people paid. Now its payroll system is safer than ever. ComputerWorld, 2008. Special Edition: p. 1-2.
10. Marcus, J., Katrina-hit campuses try to return to normal. Times Higher Education, 2007: p. 1-2.
11. *Ibid.*
12. Lumpp, T., *et al.,* From high availability and disaster recovery to business continuity solutions. Systems Journal, 2008. 47(4): p. 605-619.
13. McKinney, M., Plan before panic. Hospitals & Health Networks, 2009. 83(11): p. 35-38.
14. Shaluf, I.M., An overview on the technological disasters. DPM, 2007. 16(3): p. 380-390.
15. Bergland, H. and P.A. Pedersen, Catch regulation and accident risk: The moral hazard of fisheries' management. Marine Resource Economics, 1997. 12: p. 281-291.
16. Captial Budgets for IT hit the wall. Information Technology, 2008: p. 68.
17. Crestin, D.S., Federal regulation of new england fisheries: A different point of view. Northeastern Naturalist, 2000. 7(4): p. 337-350.
18. 3 C.F.R. ,46 FR 13193, Comp., p. 127. 1981.
19. Carlson, C., Industry poised to forestall net regulation. eWeek, 2003: p. 34.
20. Litman, J., Information privacy / information property. Stanford Law Review, 1999. 52: p.1283-1313.
21. Zalud, B., Regulations: "Golden' rules or ruling you? Security, 2009: p. 20-27.
22. Sparks, S.A., The direct marketing model and virtual identity: Why the United States should not create legislative controls on the use of online consumer personal data. Dickinson Journal of International Law, 1999. 18(3): p. 517-550.
23. *Ibid.*
24. *Ibid.*
25. Preimesberger, C., On the brink of disaster. eWeek, 2008: p. 31-38.
26. *Ibid.*
27. Mearian, L., Global firms confident about disaster recovery. Computerworld, 2003. 37(12): p. 6.
28. Martin, J. and J. Samels, 10 trends to watch in campus technology. THE CHRONICLE of Higher Education, 2007. 53(18): p. B.7.
29. Anonymous, Self-regulation plans polarise industry. The Safety & Health Practioner, 2009. 27(12): p. 8.
30. *Ibid.*
31. Jha, A., *et al.,* Safer Homes, Stronger Communities: A handbook for reconstructing after natural disasters. The International Bank for Reconstruction and Development, 2010.
32. Whitworth, P.M., Continuity of operation plans: Maintaining essential agency functions when disaster strikes. Journal of Park and Recreation Administration, 2006. 24(4): p. 40-63.

Air Mobility Command's Enterprise Information Management Program

by Chris Clements and Jim Schmitt

Hard to decipher what is the most current briefing for your Chief Executive Officer or General Officer? Want to eliminate too many versions of the same document or collaborate with others on projects? The United States Air Force (USAF) Air Mobility Command's (AMC) Enterprise Information Management (EIM) Program addresses these challenges and more.

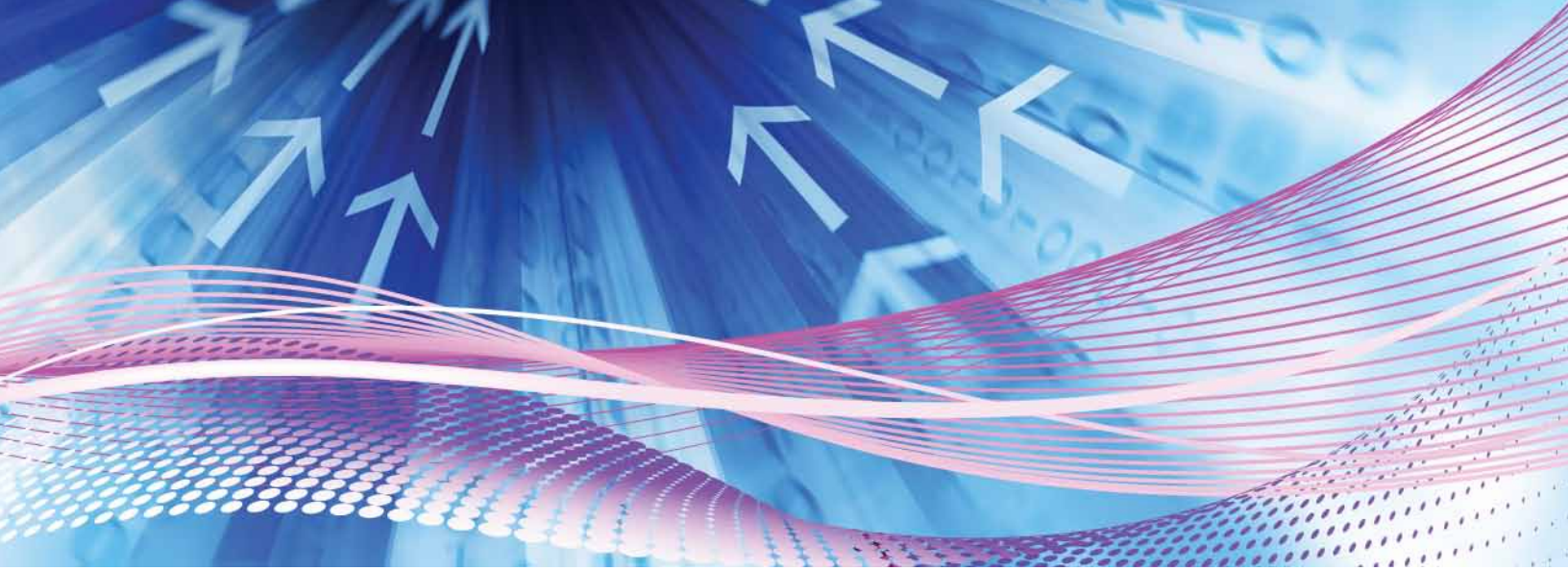
The USAF's AMC EIM Program began in June 2006 when they built a SharePoint 2003 environment to use as a pilot program for AMC's Director of Communications Operations Directorate. As with all of the products within EIM and to follow proper acquisition life cycle management, SharePoint 2003 was first tested in the Air Force Network Integration Center's Technology and Interoperability Facility to ensure it would properly operate when placed into production on the network. Since then, it has achieved the authority to operate and authority to connect through certification and accreditation of the system to both unclassified but sensitive/secret Internet protocol rooter network (NIPR Net) and (SIPR Net). The environment was upgraded to SharePoint 2007 and deployed throughout the AMC Headquarters (HQ), each of its 11 bases, HQ 18th Air Force, United States Transportation Command (USTRANSCOM), Surface Deployment Distribution Center (SDDC), Joint Enabling Capabilities Command (JECC), and the Military Sealift Command (MSC). Terabytes of structured and unstructured data were migrated from file shares and disparate Web sites/applications to a robust, enterprise-scaled EIM environment. The Secretary of the Air Force / Communications Director and Chief Information Officer (CIO) benchmarked the deployment process used by other major commands to deploy EIM throughout the USAF. From inception, the number of users has grown substantially—from its pilot program of 50 users to currently one of the largest Department of Defense (DoD) SharePoint instances that supports more than 95,000 joint personnel. EIM has ensured the timely and accurate integration of technologies including—

> The EIM system is a centralized, easy-to-use, and secure environment that enables users to execute their daily missions.

- Microsoft Office SharePoint Server (MOSS) 2007
- Microsoft Dynamics/Customer Relationship Management
- Office Communications Server (OCS)
- Hewlett-Packard's (HP) Records Management System (TRIM)
- Accenture's Task Management Tool (TMT)
- A host of custom solutions.

So what is EIM? EIM is a set of the following core disciplines leveraged to support aspects of all administrative and mission support activities: Records Management; Electronic Forms; Content Management; Knowledge Management; and Collaboration, Workflow, and Document Management. The EIM system is a centralized, easy-to-use environment that enables users to execute these disciplines in a secure environment to support their daily missions. The EIM system is an ever-evolving set of commercial off the shelf (COTS) products, government off the shelf (GOTS) products, and custom solutions. This system gains strength through its native integration with the existing USAF domains, identity management, security, and messaging systems. Additionally, most EIM components integrate directly with the standard desktop suite of products.

At the basic level, EIM allows users to access and share information in one common area online; however, it offers



much more than that. Over time, it has come to offer desktop collaboration between virtually any USAF personnel in the *.mil* domain and a workflow capability that can automatically generate, track, and route suspenses throughout all levels of the USAF. In sum, EIM can automate, to some degree, most administrative processes that USAF personnel find themselves doing every day, leaving more time to focus on the mission and less time grinding through paperwork.

The intent of EIM is not to burden users with another communications system; rather, when leveraged correctly, it will help reduce the administrative load shared by all (*i.e.,* AMC, USTRANSCOM, 18 USAF, JECC, SDDC, and MSC). EIM is a simple system that only requires its users to know how to use a mouse and keyboard and have sufficient skills to navigate a Web site—similar to using Microsoft Explorer. Even more important is the understanding that EIM is a tool for everyone to use, regardless of their job or position. Information placed in electronic environments is growing faster than ever; effectively managing the abundance of information is critical. The amount of information placed in our computers, shared drives, and Web sites can be considered a "digital landfill" that is out of control and not being managed by anyone; EIM helps get it under control. EIM streamlines processes to allow workers to do their business more efficiently. EIM, however, is not a replacement for all systems or shared drives. It is not recommended to move all content onto EIM. While Records Management is one of the core EIM disciplines, no USAF solution has been identified for the EIM environment. USAF personnel must ensure that local procedures for the storage and disposition of official records are followed.

EIM creates a virtual office where USAF personnel can access work projects from any computer with Common Access Card access—at the office, from home, or even on the road. This "virtual office" capability is a powerful benefit for the road warrior; however, it does introduce a level of risk for all who take advantage of this capability.

Safeguarding information placed on EIM is everyone's responsibility. In the past, the application and management of permissions required skilled system administrators. The primary method for addressing this risk in ELM is the implementation of access controls that are embedded in the system. With EIM, information owners have the ability to control access to the items placed on EIM. USAF personnel must become familiar with the security settings within EIM and ensure proper permissions are applied. Establishing and managing permissions is critical to protect information stored in EIM. Access controls within EIM are as flexible as they are powerful. They can be applied to whole sites, sub-sites, calendars, lists, libraries, and even specific documents. The permissions can be assigned to individuals or groups. The EIM team developed a Privacy Act/Personal Identifiable Information (PII) Guide to educate personnel and help reduce the number of PII incidents.

EIM also offers a component similar to that found on Facebook. All users can collaborate and exchange ideas from other users throughout AMC by using the MySite feature. Currently, MySites are only used to provide a personal area for users to store information unique to them. Users could easily expand them to become a professional networking resource. By standardizing the individual attributes captured on MySites, users could easily search for individuals in similar functional or mission support areas, establish professional discussion forums, or even enhance mentorship opportunities.

As outlined above, the total EIM solution is an evolving collection of COTS and GOTS products as well as custom solutions anchored by MOSS 2007. In almost all cases, the custom solutions delivered required no traditional coding. The ability to leverage custom configurations of out-of-the-box features/capabilities has reduced the total cost of development

and time to deliver these solutions. Site owners are now able to stand up capabilities on their sites that formerly would have required expensive custom development by trained programmers. This capability not only empowers information owners, but also frees up USAF programmers to focus on more complex requirements. AMC has created and cataloged numerous benchmark processes, created 11 EIM user and train-the-trainer tutorials, and new Enlisted Performance Report (EPR)/ Officer Performance Report (OPR) courses for over 132,000 personnel. The EIM team has delivered over 60 successful solutions and provided clients with huge savings such as—

- Automated the health benefit tracking process for AMC's Surgeon General and saved $97K and 160 man-hours annually;
- Provided an automated Wing deployment preparation solution that saves over 3.3K man hours per year;
- Reconfigured and consolidated multiple lists, libraries, and SharePoint groups that improved security and collaboration for McChord's Anti-Terrorism office and unit point of contacts, saving over 960 man hours a year in updating and maintaining their SharePoint site; and
- Migrated USTRANSCOM's official records management solution 3 weeks ahead of schedule.

Enterprise solutions that are built into EIM include—

- **Office Communications Server (OCS)/Office Communicator (OC)**—Enhanced real-time collaboration with AMC. Initially deployed to HQ AMC A-Staff, 18 USAF, Tanker Airlift Control Center, and Air Force Expeditionary Center, the deployment is now being extended to all AMC Wing personnel. OC provides USAF personnel with instant messaging (IM), group IM, presence, and peer-to-peer audio/video chat. In the near future, AMC will deploy enterprise OC features to a limited number of personnel throughout the command. Enterprise features will bring online conferencing, live-meetings, and group audio/video sessions. Individuals not receiving the enterprise capability will be able participate in conferences, but will not be able to initiate them.
- **AMC/Commander Visibility Balanced Scorecard**—Providing the AMC Commander visibility into critical mission indicators, the EIM team created an AMC Balanced Score Card prototype to allow senior leaders more capability to monitor organizational key performance indicators. Future iterations will utilize Enterprise SharePoint, Performance Point, and Structured Query Language (SQL), or reporting services to enhance capabilities and business analysis functions.
- **Task Management Tool (TMT)**—TMT is a solution that extends the Microsoft Customer Relationship Management platform and integrates with SharePoint. The EIM team integrated TMT into the EIM environment, providing a standardized suspense management solution for over 7,500 users across HQ AMC, USTRANSCOM, 18 USAF, and its subordinate units. AMC recently upgraded to v2.4, providing leadership with a new Senior Leader Approval Process and the ability to federate with other TMT instances. This enterprise capability has been delivered on both the classified and unclassified networks.
- **Evaluation Management System (EMS)**—Developed by Pacific Air Forces (PACAF), EMS has been adopted as a standard solution across the USAF for the processing of EPRs/OPRs, awards, and decorations. The EIM team integrated this solution into the environment and works regularly with PACAF and Air Force Space Command to improve each iteration.

What's Next?

The EIM team is jumping at the opportunity to bring EIM to the next level. They are in the pre-planning stages to upgrade AMC and USTRANSCOM's SharePoint environment to SharePoint 2010. The EIM team has also been in several high-level discussions on how to migrate AMC to a cloud computing environment that will bring the USAF up to standards within industry—they developed a Business Cost Analysis to show clients where to expect increased efficiencies. USAF senior leadership requires the need for collaboration and real-time information during contingency operations. The EIM team has delivered on a request to provide anonymous, anywhere, anytime access to authenticated users to meet operational needs in support of warfighting.

EIM continues to evolve into a more mission-essential system. As such, the EIM team is working on enhancing the redundancy of the environment for the AMC client and providing them with detailed plans to upgrade its current architecture and potentially add alternate site Continuity of Operations Plan capabilities. The team is also virtualizing much of the environment—all will be transparent to the user. They will be working closely with their counterparts in the AMC/A6 CIO division to create a strategic plan for evolving Knowledge Management practices throughout the command. The EIM team has partnered with the Air Force Network Integration Center to develop a plan for migrating OCS services to the AFNet OCS instance once established. They are working with other major commands and headquarters air force to federate the AMC TMT instance with others to enable cross command

▷ ▷ *continued on page 41*

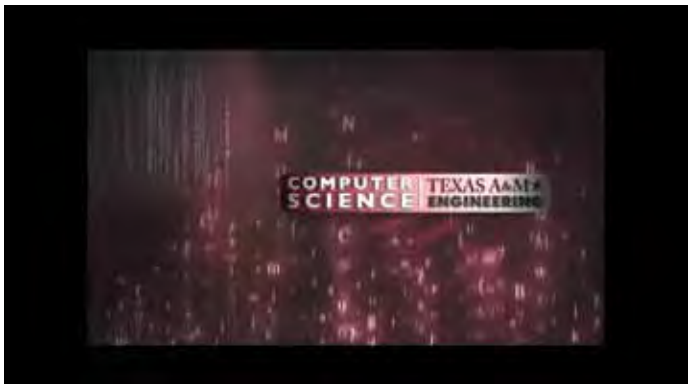
Texas A&M University

by Angela Orebaugh

Founded in 1876 in College Station, Texas A&M became Texas' first public institution of higher learning. [1] Now, Texas A&M University (TAMU) is the sixth largest university in the country and a research-intensive flagship university with over 50,000 students, 20% of them graduate students. TAMU offers 120 undergraduate and 240 graduate degree programs across 10 colleges.

The TAMU Center for Information Assurance and Security (CIAS), located in the Office of the Vice President for Research, consolidates the university's educational and research activities on information assurance and security (IAS). [2] CIAS is an organized structure for facilitating scholastic interactions of faculty and students who are actively engaged in IAS research and education by combining advanced expertise to address a broad spectrum of issues related to the expansion and protection of information and communications infrastructure systems. The National Security Agency designated CIAS as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and a Center for Academic Excellence in Information Assurance Research (CAE-R).

CIAS enhances current undergraduate and graduate information assurance (IA) courses across Computer Science, Mathematics, and Information and Operations Management departments through laboratory exercises that reinforce key concepts discussed in the classroom. Although TAMU does not offer a degree in IAS, it offers an interdisciplinary certificate program at both the M.S. and Ph.D. level. Certificate courses offer a variety of topics including e-Services, Business Information Security, Advanced Networking and Security, Data Mining, and National Security Policy. There are also opportunities to focus on IA within the Electrical Engineering and Information Management and Systems departments. [3]



Video Learn more about TAMU (Source: *http://www.youtube.com/watch?v=5DXhf_F4u4w*)

CIAS also participates in the Information Assurance Scholarship Program (IASP), which offers full tuition plus stipend for selected applications. The program is offered through the U.S. Department of Defense (DoD) IASP to increase the number of qualified students entering the field of IA to meet DoD's increasing dependence on information technology for warfighting and the security of its information infrastructure.

TAMU is hosting the 2012 Southwest Regional Collegiate Cyber Defense Competition (CCDC), which gives teams the opportunity to act as network managers by administering and protecting the team's existing commercial network against external threats. TAMU won the Regional CCDC in 2006 and the National CCDC in 2007, and took second place at Nationals in 2008. [4] ■

References

1. *http://www.tamu.edu/about/facts/*
2. *http://cias.tamu.edu/*
3. *http://cias.tamu.edu/education*
4. *http://ccdc.tamu.edu/*

Accurately Projecting IA Costs

by William T. Bailey

I began my career as a design engineer when three-legged transistors were the basic electronic building block. Over the last 10 years, I have worked on many programs that made a critical mistake—the information assurance (IA) budget was virtually nonexistent. In my worst experience, I was the Information Assurance Manager (IAM) on a multi-billion dollar program to help lead the IA team to achieve an authorization to operate (ATO). I started after the program was underway, and management had already begun working with non-IA personnel who did not understand the importance of an ATO. I inherited an original budget "cast-in-concrete," and the time allocated to do the IA project was significantly underestimated. There was an unbelievable amount of friction, both by management as well as design engineers, regarding the mandatory requirements of the 8500 series IA compliance. I spent the next year trying to educate the team and principal design engineers on "mandatory" IA controls and "rule-sets." While the program stayed on schedule, the budget remained an ongoing battle.

In retrospect, the real problem was that the budget did not adequately account for all of the IA requirements identified in the contract; the original budget was developed without a clear understanding that IA compliance was a mandatory requirement. Even now, industry develops cost and technical proposals without an IA professional's input.

This article explains why there can be IA issues when assessing project costs, and examines security environments where contract misunderstandings and costly errors are very likely to occur. I conclude with how to avoid making these costly errors.

Understanding Enterprise vs. Tactical IA

According to *Dictionary.com*, cybersecurity refers to the state of being "safe from electronic compromise." [1] IA often refers to the measures taken to achieve a state "safe from electronic compromise" (*i.e.,* cybersecurity). Although the buzzword currently is cybersecurity, keep in mind that the cybersecurity building blocks are made up of confidentiality, integrity, availability, authentication, and non-repudiation, which are the five pillars of IA.

To achieve cybersecurity, the security implementation process must be clear, predictable, and repeatable; therefore, to assure consistency in the security design approach, one must use a standard implementation baseline governing the targeted security environment. The starting point is the fundamental baseline reference called the Application Security and Development, Security Technical Implementation Guide (STIG). [2] Developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD), this STIG represents one of many security documents defining IA governance and requirements in building and operating within the Global Information Grid. [3]

Principal to cybersecurity implementation is the DoD IA 8500 series of documents (*i.e.,* the foundation of IA security). The term IA is relatively new [4], but the guidelines are not; they come from the primary security reference, the Orange Book. [5] Its requirements are clearly delineate between two major types of IA security: the enterprise environment and the tactical environment. As much as the requirements fall into these two distinctly different security environments, there remains some confusion as to which is an IA requirement...they both are.

Each requirement is specifically applicable over its security domain in accordance with the contract requirements. The two levels of responsibility—enterprise and tactical—are essentially two entirely different worlds of security, both following the Orange Book requirements. A very large number of IA practitioners are enterprise-specific personnel, and have never had the opportunity to work or understand a mandatory tactical environment. Often, the differences between the two are specified within

government contract requirements; the contract may either specify a Mandatory Access Control (MAC) category security requirement, which indicates an IA tactical environment, or a Discretionary Access Control (DAC) category security requirement, which indicates an IA enterprise environment.

A tactical environment (MAC) governs a warfighter's interactive security environment through sensors, weapons, communication equipments, countermeasures, and physical engagement. A tactical environment may also include training, such as the simulation of airborne or ground and maritime computer generated forces of a virtual battlefield. To improve training proficiency and response time, the trainer coordinator can interactively alter scenarios by controlling computer generated forces, resulting in richer exercise content in terms of tactical situations. Just to reiterate, a MAC is always a mandatory IA control implementation requirement.

An enterprise environment (DAC) is generally all security environments other that tactical. This environment covers industry's proliferation of networks as well as U.S. government executive branch departments and agencies. The operation security level, sometimes classified, falls under the National Industrial Security Program Operating Manual, where contractors establish internal procedures as necessary (*i.e.,* the contractor prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information). This is an environment of discretionary governance (DAC) even though it may be designed with governing IA compliance requirements. The security level, which is enforced by the IA compliance requirements, under the DAC may require a complete IA compliance configuration. The key point here is that the enterprise environment is not held to the same standards as a tactical environment (MAC), where contractors must protect all classified information to which they have access or custody. The contractor rule-set is to perform DAC security within the confines of a federal installation and safeguard classified information according to the procedures of the host installation or agency.

Keep in mind that the MAC category is a level of ultimate security. That means that once defined, it is an independent variable that remains the same throughout the program's life. On the surface, MAC and DAC appear distinguishable and separate.

Understanding Additional Security Considerations

The same acronym, MAC, is used for a different term by the government in contract requirements; it specifies a security level of compliance as a contractual obligation. This contractual selection category is called a Mission Assurance Category (MAC) requirement, consisting of three contract level choices, where only one is defined per contract—

- **MAC I**—Fundamentally covers information that is vital to the operational readiness as well as consequential to the loss of mission effectiveness;
- **MAC II**—Important to the support of deployed and contingency forces and loss of availability; and
- **MAC III**—Does not materially affect support to deployed or contingency forces. [6]

From these definitions, MAC-III is considered a low level of risk and MAC-I is a high level of risk; however, the MAC risk level alone is not sufficient to fully identify the contract requirements. The personnel who are permitted to work on the system must also be subjected to a mandatory level of confidentiality; therefore, one can see that a Confidentiality Level (CL) also influences the applicability of a DoD information system.

The CL is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations as well as interconnection controls and approvals, and acceptable methods by which users

may access the system (*e.g.,* intranet, Internet, wireless). Typically, the program manager will define the MAC and CL for the program.

The MACs define the risk elements, but not necessarily the security requirements. The security categories are expanded to include a CL (*i.e.,* MAC/CL), where the CL is actually a requirement for a personnel security level. The DoD has three defined CLs: Classified, Sensitive, and Public. Classified systems process classified information; Sensitive systems process sensitive information as defined in DoDD 8500.01E (to include any unclassified information not cleared for public release); and Public systems process publicly releasable information as defined in DoDD 8500.01E (*i.e.,* information that has undergone a security review and been cleared for public release).

The government program manager typically creates a security classification guide (in accordance with APP2040.1) if the system contains classified information. Also, the program manager defines the MAC and CLs for the program. For example, a typical training simulator may be categorized as a MAC-III/CL Sensitive. Tables 1 and 2 provide several options available to define an overall system security requirement.

Mission Assurance Category Levels for IA Controls			
MAC	**Definition**	**Integrity**	**Availability**
1	These systems handle information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.	High	High
2	These systems handle information that is important to the support of deployed and contingency forces.	High	Medium
3	These systems handle information that is necessary for the conduct of day-to-day business, but does not materially affect suppor to deployed or contingency forces in the short-term.	Basic	Basic

Table 1 MAC levels for IA control

Confidentiality Levels for IA Control	
Confidentiality Level	**Definition**
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoDD 8500.01E (to include any unclassified information not cleared for public release)
Public	Systems processing publicly releasable information as defined in DoDD 8500.01E (*i.e.,* information that has undergone a security review and been cleared for public release)

Table 2 CLs for IA control

Best Practices for Accounting for IA and Security in a Contract

The following example will demonstrate the confusing thought process one might follow while trying to understand the MAC/CL requirement. If the requirement is "MAC-I/CL Public," the nomenclature would identify a high level of operability and a low level of personnel security (*i.e.,* a high level of system expenditure and a low level of investment protection).

Even though the program MAC/CL are typically defined in the contract requirements for an IA requirement, the MACs/CLs are not typically addressed in the statement of work (SOW). The information about mandatory or discretionary (MAC/DAC) data is typically understood to be defined by information found in the SOW. When the SOW specifically references the IA or the DoD 8500 series, it is a mandatory requirement. If the contract does not specifically mandate IA requirements, it is not a tactical requirement; if it is not a MAC, it has to be a DAC since the Orange Book only addresses these two top-level categories. From a legal viewpoint, however, if you know a "new" contract requires IA, but the design fails to include IA, you are in for a surprise; the government requires contractors to perform technical IA work with "Due Care," meaning in accordance with standard IA doctrine (*e.g.,* DoD 8500 series).

The IA requirements in proposal development efforts require establishing a project budget to include all IA tasks to be performed as well as the cost allocation for personnel security levels working on the budgeted tasks. A word of caution in proposal development—be very attentive to IA requirements when responding to a Request for Proposal for government design and development. The rule is that new government contract expenditures require IA compliance on any new project as well as on any new upgrade components to legacy projects. The cost estimates must, therefore, ensure that a discrete line item for IA is established in

programming and budget documentation at the beginning of the development effort.

If the contract or SOW has any mention or reference to IA, the cost of development can go up considerably. Only an IA practitioner knows what the full extent of the IA requirements may be, and only an IA practitioner should build a proposal's Basis of Estimate. If the contract or SOW references IA compliance, the security door may be wide open for the government IA manager to misinterpret the requirements as a completely IA compliant system. Keep in mind, the IA control elements consist of 157 IA controls, and you only want to satisfy the ones specific and relevant to your program. To assure cost containment, a System Requirements Traceability Matrix is imperative to develop up-front, before misunderstandings start to occur. This is necessary because IA is a cradle-to-the-grave responsibility, and "full-up" IA compliance includes system development life cycle implementation, configuration control, software upgrade loading, DoD Information Assurance Certification and Accreditation Process (DIACAP) documentation, and certification and accreditation testing. ■

About the Author

William T. Bailey | is an IA analyst for the Camber Modeling, Simulation, and Training Division in Huntsville, AL. He provides IA management and leadership regarding IA proposal and tactical requirements as well as DIACAP/ATO security compliance and implementation processes. He is completed a Ph.D. program at California Coastal University (1990) and is a Doctoral Candidate level in IA at the University of Fairfax (2012). Early on, he was the Director of Operation for CONTEL. He can be contacted at *iatac@dtic.mil*.

References

1. *http://dictionary.reference.com/browse/cybersecurity?o=100083&qsrc=2894&l=dir*
2. Application Security and Development. Security Technical Implementation Guide, Version 2, Release 1, 24 July 2008, *http://www.databasesecurity.com/dbsec/database-stig-v7r1.pdf*.
3. *http://iac.dtic.mil/iatac/ia_policychart.html*
4. Bluth, A & Kovacich G, (2006) Information Assurance in the Information Environment, Springer-Varleg, London Limited.
5. *http://www.dynamoo.com/orange/summary.htm*
6. DoDI Number 8500.2, February 6, 2003, Enclosure 4, *http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf*

▷ *continued from page 11*

DAMAGES FROM CYBER ATTACKS

Institute at Carnegie Mellon University. He has applied operations research models in a number of areas including policy analysis, telecommunications, and technology management. He is currently working on various aspects of network sensors, network traffic analysis, and workflow models. He can be contacted at *smoitra@cert.org*.

References

1. Moitra, S. D. Evaluating the Benefits of Network Security Systems. *IAnewsletter*, Vol. 14, No. 4, Fall 2011, pp 42-46.
2. Arora, A. *et al.* – Measuring the risk-based value of IT security solutions. IT Professional , vol.6, no.6, pp. 35- 42, Nov.-Dec. 2004.
3. Brotby, W. K. – Information security management metrics: a definitive guide to effective security monitoring and management. CRC Press, Boca Raton. 2009.
4. Gordon, L.A. and Loeb, M.P. Managing Cybersecurity Resources. McGraw-Hill, New York, 2006.
5. Hoo, K. J. S. "How Much Is Enough? A Risk-Management Approach to Computer Security." Working paper, Consortium for Research on Information Security and Policy (CRISP), June 2000.
6. Paquet, C. and Saxe, W. The Business Case for Network Security: Advocacy, Governance and ROI. Cisco Press, 2004.
7. ANSI – The Financial Impact of Cyber Risk. 2008.
8. D'Amico, A. D. What does a Computer Security breach Really Cost? Secure Decisions, 2000.
9. McQueen, M.A., Boyer, W.F., Flynn, M.A., Alessi, R.S., "Quantitative risk estimation tool for control systems: suggested approach and research needs". International Workshop on Complex Network & Infrastructure Protection (CNIP 06), Rome, Italy. March 28-29, 2006. Idaho National Laboratory Technical Report INL/CON-06-01255.
10. Smith, G. S. "Recognizing and Preparing Loss Estimates from Cyber-Attacks." Information Security Journal: A Global perspective, Vol. 12, Issue 6, pp. 46-57. 2004.
11. CSI (Computer Security Institute) – "CSI Computer Crime and Security Survey 2009."
12. Ponemon Institute. 2010 Annual Study: US Cost of a Data Breach, 2011.
13. Rantala, R. R. "Cybercrime against Businesses, 2005." Special Report, Bureau of Justice Statistics. Office of Justice Programs, U.S. Department of Justice. September 2008.
14. Karabacak, B. and Sogukpinar, I. "ISRAM: Information Security Risk Analysis Method." Computers & Security, Vol. 24, Issue 2, pp. 147-159. March 2005.
15. *Ibid.* (see reference 1)
16. Layton, T. P. Information Security: Design, Implementation, Measurement, and Compliance. Aurbach Publications, 2006.
17. Shostack, A. and Stewart, A. The New School of Information Security. Addison-Wesley, Upper Saddle River, NJ, 2008.
18. *Ibid.* (see references 3,4,5,6,7)
19. Moitra, S. D., Assessing the Benefits and Effectiveness of Network Sensors. 2010 CERT Research Report. CERT, SEI, Carnegie Mellon University, 76-78, 2011.

Ask the Expert

by Ed Moyle

Why Data Expansion Matters for IA

It is a truism that technology use increases over time. Until recently, the mechanics of how that increase happens was static; however, these processes are evolving, and as they do, changes in how new technology is deployed have pretty serious implications for information assurance (IA) professionals. IA professionals should understand how this shift occurs and plan accordingly.

Why Technology Growth is Changing

We are all very familiar with the model of outward-expansion that has occurred in most organizations; in response to organizational, mission, and technology requirements, information technology shops have deployed new hosts/devices while replacing existing ones as needed. Everything from workstations to servers, from mobile devices to networking components, were layered upon each other to keep pace with updates to technology standards.

Recently though, technology expansion has started to follow another pattern: an inwardly-directed expansion in addition to outward-facing expansion. What this means is that in addition to layering new devices into the environment, technology that we have already fielded is also starting to become more densely populated with critical and sensitive data.

Consider, for example, efforts like datacenter consolidation, server virtualization, and private cloud. These technologies all have one thing in common—they consolidate resources. They all serve to bring previously far-flung technology components to the core of the infrastructure and to centralize them there. In the past, one physical host might host an application or two (maybe a database). In a virtual world, that same device might be hosted centrally as a virtual resource along with numerous other virtual instances. In the past, resources were gated by the physical hardware on which they ran. Now the only thing gating expansion is storage capacity, which is a nearly limitless upper bound.

Implications for IA

For IA professionals, this has some serious implications. In the near term, it means we need to revisit our risk analyses because increasing the volume of data at the core can mean higher risk in the event the infrastructure is compromised. IA professionals, therefore, may need to revisit their countermeasures in light of broader risk and higher impact.

In the intermediate term, IA professionals need to re-look at the controls they have already fielded and ensure they operate effectively as data density increases. For example, consider a control like data discovery aspects of data loss prevention. A linear search through a small volume of data (*e.g.*, terabyte) to ensure it is stored appropriately might take only a few minutes. What about when the volume expands to exabytes or more? Searching that data once, let alone repeatedly, is a whole magnitude of difficulty greater, so this control might not make sense.

Lastly, in the long term, certain controls are easier to add before data volumes get cumbersome. Consider bulk-encrypting data—encrypting an exabyte of data is computationally expensive. It is much easier to encrypt in small increments (*e.g.*, encrypting data additively as it is created). In other words, structuring the control to grow with the data is easier in the long run.

The world is changing; therefore, our efforts in IA have to change with it. For organizations that seek to make the most of security controls to best support the mission, it makes sense to think through—both short- and long-term—how changes in data size play out in light of existing controls. ■

About the Author

Ed Moyle | is a 15+ year veteran of information security as well as an industry-recognized thought leader, advisor, writer, and manager. Mr. Moyle is currently a faculty member at IANS, Senior Security Strategist with Savvis, and a founding partner of SecurityCurve. He can be contacted at *iatac@dtic.mil*.

tasking and workflow. These efforts will also turn to testing and fielding the latest version of the Enlisted Management System in March 2012.

Once all capabilities are deployed and fully configured, everyone will be encouraged to take maximum advantage of its benefits. AMC HQ A6 Director of CIO, the EIM team, and AMC Communications Squadrons will continue to work hard to help users get the most out of EIM now and in the future. ■

About the Authors

Chris Clements | is an IT professional with an M.S. in Information Technology Management and over 23 years of experience in a range of competencies including system administration, application design and development, enterprise system implementation, and program management. An Air Force retiree. Mr. Clements has supported EIM for both Air Force Network Integration Center (AFNIC) and AMC, the AFNet OCS deployment, and the USTRANSCOM migration to the AMC classified domain. He can be contacted at *iatac@dtic.mil*.

Jim Schmitt | is the Air Mobility Command's EIM Task Lead. He has over 27 years of experience working with the DoD in the communications field at various levels culmination in functional management. As an Air Force retiree, he has worked Process Improvement Efforts for the AFNIC as well as his current task as EIM Task Lead. Mr. Schmitt has supported EIM for both AFNIC and AMC, oversaw AFNet OCS deployment, and the Joint Enabling Capabilities Command migration to the AMC classified domain. He is currently leading the shutdown of the AMC-2K Legacy domain and standing up the same SharePoint Farm in the AFNet…an Air Force first. He can be contacted at *iatac@dtic.mil*.

Letter to the Editor

Q The winter 2012 edition of the *IAnewsletter* featured an article titled "Securing the Mobile Device…and its User." I am interested in how the Department of Defense (DoD) has responded to the need to secure mobile devices. What DoD policies and guidance have been issued on this topic?

A The following DoD policies and guidance are a sampling of what has been issued to secure information on mobile devices.

In April 2006, DoD issued a memorandum on "Protection of Sensitive Department of Defense Data at Rest on Portable Computing Devices" that recognizes the need to insure that DoD information on mobile device hard drives remains protected, especially in the event that a device is stolen or misplaced. This policy stresses the importance of encrypting data on the hard drives whenever possible, implementing identity and authentication controls, and using passwords to manage access to encrypted and unencrypted data. [1]

In July 2007, DoD issued a memorandum on "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," which takes the April 2006 guidance one step further. This policy mandates that all unclassified DoD data not publicly releasable be encrypted using technologies that meet National Institute of Standards and Technology Federal Information Processing Standard 140-2. [2]

DoD recognizes the need to provide policy guidance for commercial technologies, too. The DoD Directive 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid," and DoD Instruction 8420.01, "Commercial Wireless Local-Area Network Devices, Systems, and Technologies," recognize the need to grant users greater flexibility in using commercial technologies while also ensuring the proper controls are in place to protect DoD information. [3, 4]

Overall, DoD policy and guidance for securing mobile devices recognizes the benefits that mobile devices provide, while also ensuring reasonable controls are established to prevent against information leaks and threats. ■

References

1. *https://www.rmda.army.mil/privacy/docs/foia-DoDSctyGuidPortableComputers.pdf*
2. *http://www.doncio.navy.mil/Download.aspx?AttachID=288*
3. *http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf*
4. *http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf*

DoDTechipedia Happenings

by Sandy Schwalb

For a number of years, the Information Assurance Technology Analysis Center (IATAC) has offered a space in its *IANewsletter* to provide an update on DoDTechipedia "happenings." As we bid farewell to IATAC, this gives us one last opportunity to report on where DoDTechipedia is today.

A wiki aimed at the Department of Defense (DoD) research and engineering community, DoDTechipedia was launched in October 2008. Mr. Al Shaffer, Principal Deputy, Assistant Secretary of Defense, Research & Engineering (ASD [R&E]), has called DoDTechipedia, "the power of the collective mind." The wiki offers a place to tell your project's story, update articles, and build and share information. DoDTechipedia continues to evolve according to the needs of its user community. Since it is a wiki, the information is not static. You can add your insight to pages or articles posted or create new ones, view tutorials, sign up for training, or join an online webinar.

Check out the *News and Events* page to get up-to-date Science & Technology news; it has articles from the Armed Forces Press Service, DoD news releases and podcasts from the White House and Science Daily, and upcoming events—all in one place.

Continue to watch for current news articles from major media outlets through "In the News," which provides links to material already posted in DoDTechipedia as well as the Defense Technical Information Center's (DTIC's) collection. If you are a subject matter expert or want to learn more about the news topics, you can share your insights and/or questions. Topics are added on a regular basis or updated as needed. All of this material is archived on DoDTechipedia: *http://www.dtic.mil/dtic/announcements/DoDtechipedia.html*.

Some topics recently highlighted include—

- **Smart Bullets**—Rather than being confined to a ballistic trajectory, they can turn, speed up, slow down, even send data back to their masters.
- **Snakebots**—Continuum robots have characteristics that make them suitable for many tasks.
- **Gaming**—Games and simulations are being used in military training.
- **Anti-Access, Area Denial**—Techniques to deter, delay, or disrupt force projection.
- **Body Armor**—New research is resulting in new approaches to personal protection.

DoDTechipedia 101 Webinar

DTIC offers a monthly webinar on DoDTechipedia using Defense Connect Online. These webinars provide a general overview to get you started on DoDTechipedia, how to add content, create your personal space, and navigate the wiki. Go to *https://www.dodtechipedia.mil/dodwiki/x/UIE6Aw* for more information on how to participate in these webinars.

Please continue to share your knowledge, assist a colleague, ask a question, post an event, start a blog, and be part of DoDTechipedia's knowledge network. To ensure that the most advanced technologies reach the warfighter tomorrow, collaborate on DoDTechipedia today.

Let Your Voice Be Heard

Are DTIC services meeting your needs? Let us know through our online feedback form: *DTIC CARES*. ■

DoDTechipedia is a project of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Assistant Secretary of Defense, Research & Engineering; the Defense Technical Information Center; and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Office.

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online: *http://www.dtic.mil/dtic/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ☐ USA ☐ USMC ☐ USN ☐ USAF ☐ DoD ☐ Industry ☐ Academia ☐ Government ☐ Other

Please list the Government program(s)/project(s) that the product(s) will be used to support: _____

_____

LIMITED DISTRIBUTION

IA Tools Reports ☐ **Firewalls** ☐ **Intrusion Detection** ☐ **Vulnerability Analysis** ☐ **Malware**

Critical Review and Technology Assessment (CR/TA) Reports
- ☐ Biometrics (soft copy only)
- ☐ Configuration Management (soft copy only)
- ☐ Defense in Depth (soft copy only)
- ☐ Data Mining (soft copy only)
- ☐ IA Metrics (soft copy only)
- ☐ Network Centric Warfare (soft copy only)
- ☐ Wireless Wide Area Network (WWAN) Security
- ☐ Exploring Biotechnology (soft copy only)
- ☐ Computer Forensics (soft copy only. DTIC user code MUST be supplied before this report is shipped)

State-of-the-Art Reports (SOARs)
- ☐ Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain (DTIC user code must be supplied before this report is shipped)
- ☐ Measuring Cybersecurity and Information Assurance
- ☐ The Insider Threat to Information Systems (DTIC user code must be supplied before this report will be shipped)
- ☐ A Comprehensive Review of Common Needs and Capability Gaps
- ☐ Software Security Assurance
- ☐ IO/IA Visualization Technologies (soft copy only)
- ☐ Modeling & Simulation for IA (soft copy only)
- ☐ Malicious Code (soft copy only)
- ☐ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletter hardcopies are available to order. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 12	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 13	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 14	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 15	☐ No. 1			

SOFTCOPY DISTRIBUTION

The following are available by e-mail distribution:

- ☐ IADigest
- ☐ Research Update
- ☐ Cyber Events Calendar
- ☐ Technical Inquiries Production Report (TIPR)
- ☐ IA Policy Chart Update
- ☐ *IAnewsletter* (beginning in Spring 2012)

Fax completed form to IATAC at 703/984-0773 or order online at: http://iac.dtic.mil/iatac/form.html

Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

Calendar

May

DISA Mission Partner Conference
7–10 May 2012
Tampa, FL
http://www.afcea.org/events/

Joint Warfighting Conference 2012
15–17 May 2012
Virginia Beach, VA
http://www.afcea.org/events/jwc/11/intro.asp

IEEE Symposium on Security and Privacy
20–23 May 2012
San Francisco, CA
http://www.ieee-security.org/TC/SP2012/index.html

TechNet Europe 2012
30–31 May 2012
Prague, Czech Republic
http://www.afcea.org/europe/html/TNE12Home.htm

June

AFCEA Technology & Industry Day
14 June 2012
Tacoma, WA
https://ca.dtic.mil/pubs/survey/caressuiteofservices1.htm?path=/pubs/survey/

Global Intelligence Forum
20–21 June 2012
Denver, CO
http://www.afcea.org/events/globalintelforum/12/welcome.asp

July

TechNet Land Forces: Joint and Coalition Issues
9–12 July 2012
Tampa, FL
http://www.afcea.org/events/tnlf/

BlackHat USA 2012
21–26 July 2012
Las Vegas, NV
http://www.blackhat.com/usa/

August

21st USENIX Security Symposium
8–10 August 2012
Bellevue, WA
http://static.usenix.org/event/sec12/

TechNet Land Forces: Cyber
13–16 August 2012
Baltimore, MD
http://www.afcea.org/events/tnlf/

GFIRST 8
19–24 August 2012
Atlanta, GA
http://www.us-cert.gov/GFIRST/

AFITC 2012
27–29 August 2012
Montgomery, AL
http://afitc.gunter.af.mil/

DoD IA Symposium
28–30 August 2012
Nashville, TN
http://www.informationassuranceexpo.com/

To change, add, or delete your mailing or e-mail address (soft copy receipt), please contact us at the address above or call us at: 703/984-0775, fax us at: 703/984-0773, or send us a message at: *iatac@dtic.mil*