GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

Los Alamos
NATIONAL LABORATORY
EST. 1943

LA-UR-14-28551
Approved for public release; distribution is unlimited.

Title:	That's where the Data is! Why Break into the Office of Personnel Management Systems - Because That Is Where the Sensitive Information for Important People Is Maintained!
Author(s):	Belangia, David Warren
Intended for:	Paper for Graduate Program at STI
Issued:	2014-11-03

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

© 2014 SANS Institute, Author retains full rights.

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer,is operated by the Los Alamos National Security, LLC for the National NuclearSecurity Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Departmentof Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

© 2014 The SANS Institute Author retains full rights.

That's where the Data is! Why Break into the Office of Personnel Management Systems - Because That Is Where the Sensitive Information for Important People Is Maintained!

GIAC (GSLC) Gold Certification

Author: David W. Belangia, dwbelangia@hotmail.com
Advisor: Stephen Northcutt

Accepted: September 30th 2014

Abstract

The place to get sensitive information relating to people who have access to our country's most sensitive information is the Office of Personnel Management's e-QIP Databases. These repositories provide a single location that contains the complete history and all associated pertinent information for anyone with a security clearance. There was a cascading failure of controls that led to the compromise identified by the New York Times in July 2014. Attackers only require a single vulnerability to obtain a foothold from which to compromise the environment. The concept of defense-in-depth is especially important for protecting sensitive information. Encryption of data at rest and in transit would have rendered the compromise useless by eliminating the ability of the attacker to use the information. All controls could have failed but the reward for the attacker would have been useless with a proper implementation of Control 17: Data Loss Prevention.

© 2014 The SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

Introduction

To obtain the most complete information about American personnel who have security clearance, an adversary would clearly be interested in compromising the information being collected by the Office of Personnel Management (OPM). The aggregation of information about an individual and their life history is collected and maintained by this organization and available in one place.

In the United States, the Privacy Act of 1974 (As Amended) "describes the challenge for privacy for electronic records" (Herrmann, 2007, p.262). The Act laid out 5 principles to include: 1) privacy is directly affected by processes associated with collection, maintenance, use and dissemination by Federal agencies; 2) Increasing use of computers is essential to efficient operations and greatly increases the potential for harm; 3) opportunities for secure employment, insurance, and credit are endangered by misuse; 4) right of privacy is fundamental and protected by the Constitution; and 5) Congress must act to regulate collection, maintenance, use and dissemination.

The Ponemon Institute has provided an annual report on the cost of data breaches for nine years. The 2014 report was a joint effort by the Ponemon Institute and IBM. The report is based on 314 global companies representing 10 countries who experienced a loss or theft of Personally Identifiable Information (PII). The costs reported are extrapolated from actual data loss incidents. The Ponemon report advises the average cost increased by 9 percent to $201 per record in 2013 (Ponemon, 2014).

On July 9, 2014, the New York Times (NYT) published an article entitled "*Chinese Hackers Pursue Key Data on U.S. Workers*" (Schmidt, Sanger, Perlroth, 2014) providing one of the first published accounts of an attack by hackers into computer networks managed by the Office of Personnel Management (OPM) that occurred in the March time frame. While the NYT reports that the OPM advises that no loss of personally identified information has been identified, this should not provide any level of comfort for a cleared individual. Recent attacks on the Department of Energy (DoE) prompted DoE management to initially advise this same line of reasoning but eventually

© 2014 The SANS Institute Author retains full rights.

disclosed that the data of 104,179 employees was compromised (U. S. Department of Energy, 2013).

The OPM is responsible for the conduct of background investigations for prospective and current employees across the government. Every security clearance is tracked by this organization. A 2013 Report on Security Clearances Determinations published by the Office of the Director of National Intelligence states that as of October 1, 2013 there were 3,091,977 individuals eligible for access to classified information (Office of the Director of National Intelligence, 2014). This is a substantial quantity of potential targets for identify thief and/or more lucrative leveraging of clearance information.

To make matters worse, the amount of personal information collected is staggering. The Questionnaire for National Security Position Standard Form 86 (2010) is 127 pages of information required by an applicant. Included is this form is all the information about the individual, their family, their education, their work experience, military experience, criminal information, and additional information about everyone in their family. The amount of information aggregated in this one form ensures that its theft could easily compromise them and potential any family member's identity.

The average per capita cost of a data breach is estimated at $195 per record within the United States according to the most recent Ponemon research (Ponemon, 2014, p. 5) The Ponemon report calculates the average costs of a data breach by quantifying direct expenses (consulting, support, credit monitoring, legal defense, etc...) and indirect expenses (existing labor involved, potential customer loss, etc…). If you assume even 10% of OPM's available records were compromised that would equate to an anticipated cost of $60,293,552 (3,091,977 x 10% x $195 per account). This is a substantial expense excluding the negative publicity relating to trusting an agency with this much vital information about an employee or contractor.

The SANS Institute working with several US Government organizations developed a Consensus Audit Guideline (CAG) or Twenty Critical Security Controls for Effective Cyber Defense (Consensus Audit Guidelines) in response to data loss experiences by US government and commercial organizations. The CAG provides a

© 2014 The SANS Institute Author retains full rights.

prioritized roadmap of controls allowing an organization to concentrate on key controls in a fashion appropriate for their environment.

Critical Security Control 17: Data Protection is the key control that would have prevented or minimized this compromise. This control is best achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques (Tarala, Cole, 2014). The OPM was relying on defense-in-depth to protect the sensitive information and over time industry will learn of multiple failures that lead to the loss of this information. A mixture of the 15 suggestions for implementing Critical Security Control 17 would have provided a final secure approach that after all other controls failed would have rendered the attack useless.

Important aspects of the Critical Security Control 17 that will be discussed in this paper include: (CSC 17-1) deploy encryption on mobile devices and systems that hold sensitive information; (CSC 17-2) ensuring encryption uses vetted algorithms; (CSC 17-3) perform an assessment to identify sensitive information; (CSC 17-7) employ encryption when moving data; and (CSC 17-11) perform an annual review of algorithms. Implementing cryptography provides confidentiality, integrity, authentications, and non-repudiation. (Conrad, Misenar, Feldman, 2012, p. 244)

According to urban legend, the famous gangster, Willie Sutton, once said he robbed banks because that's where the money is. Why would someone break into the OPM? It is because that is where the sensitive information relating to people who have access to our country's most sensitive information resides.

Controls fail! The concept of defense-in-depth is designed to provide additional layers of protection to accommodate these failures. The proper implementation of Critical Control 17 would render all other failures useless as the perpetrator would only steal information that could not be used. When this control is applied properly, sensitive information would be secure as required by the Organization for Economic Cooperation and Development (OECD). The OECD provides 8 privacy principles. Principle 5: Security Safeguards, advises that information must be protected by reasonable safeguards (SANS, 2011. p. 218). This additional control provides the final security safeguard to prevent a compromise of the enterprise from becoming a data breach. The cost of

© 2014 The SANS Institute Author retains full rights.

mitigating a data breach is expensive, time consuming, and damaging to the enterprise's reputation.

1. Requirements for Protection

1.1. Law

There are five primary International guidelines and/or regulations that provide the principle focus on the protection of security and privacy associated with PII. They are: 1) the Organization for Economic Cooperation and Development (OECD) Privacy, Cryptography, and Security Guidelines; 2) Directive 95/46/EC Data Protective; 3) the Data Protection Act – United Kingdom; 4) the Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada; and 5) the Privacy Act – United States. (Herrmann, 2007, p. 212).

All five share surprising similar attributes to include collection, integrity, stated purpose, use limitations, individual's rights, and protection. They strive to allow the use of this information as it is recognized that for free commerce to work, this is required. Most countries share a similar desire to protect the individual while allowing the required processing of this information. The rapid advance of technology further complicates the situation.

The United States and other countries have made multiple attempts at defining sensitive information, providing guidance on protection, and limiting the information that can be collected. The Privacy Act laid out 5 principles to include: 1) privacy is directly affected by processes associated with collection, maintenance, use and dissemination by Federal agencies; 2) Increasing use of computers is essential to efficient operations and greatly increases the potential for harm; 3) opportunities for secure employment, insurance, and credit are endangered by misuse; 4) right of privacy is fundamental and protected by the Constitution; and 5) congress must act to regulate collection, maintenance, use and dissemination.

© 2014 The SANS Institute Author retains full rights.

The United States has attempted to provide additional guidance and requirements through the Federal Information Security Management Act (FISMA), Homeland Security Presidential Directives (HSPDs), the North American Electrical Reliability Council (NERC) Cyber Security Standards, and the Patriot Act. These documents are an attempt at solving identified issues while trying to keep pace with exploding technology advancements. It certainly is a fight worth fighting but we are losing the battle!

As Hermann states, "many authorities have taken the position that an individual's right to privacy must be sacrificed to ensure the physical safety of the public at large" (Herrmann, 2007, p 351). With the concerns about terrorist attacks and the recent Snowden disclosures, national attention is again being focus on personal rights, collection of information, subsequent use and protection. There will be more regulations and/or help coming to the industry from well-intentioned legislators.

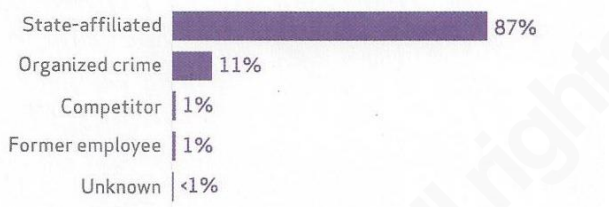
1.2. The Problem

Ponemon working with IBM published the ninth annual *Cost of Data Breach Study: Global Analysis*. This study highlighted a 9% increase in the average cost associated with a data breach to a average magnitude of $3,500,000. This study represented 314 companies in 10 countries. Each company had experienced a data breach ranging in magnitude from 2,415 to over a 100,000 compromised records. The Ponemon report calculates the average costs of a data breach by quantifying direct expenses (consulting, support, credit monitoring, legal defense, etc...) and indirect expenses (existing labor involved, potential customer loss, etc…). The cost of a data breach is estimated at an average of $195 per record within the United States (Ponemon, 2014).

Cyber espionage information is not reported as freely and attribution is difficult to make. Organizations are not required to publicly disclose information relating to these cyber espionage attacks unless they include the compromise of PII. The *Annual Data Breach Investigation Report* published

© 2014 The SANS Institute Author retains full rights.

by Verizon provides on an annual basis statistics relating to cyber espionage using information from actual compromises. From 2013 to 2014, Verizon estimates that the number of incidents tripled from the already increasing number the previous year. Verizon provides detailed analysis providing insights into the attributes of the problem. The variety of actors was characterized as 87% state affiliated of which 49% were from Eastern Asia. The major avenue used in their attacks included email attachments and web drive by attacks (Verizon, 2014). This is the most likely entry point in the OPM incursion.



2. Office of Personnel Management Compromise

2.1. Who Was Affected?

The July 9, 2014 NYT article entitled "*Chinese Hackers Pursue Key Data on U.S. Workers*" was a wakeup call and provided information relating to an attack by hackers into computer networks managed by the OPM. OPM is advising they are unsure if any PII was compromised. This is very reminiscent of the Department of Energy (DoE) where eventually DoE disclosed that the data of 104,179 employees was compromised (U.S. Department of Energy, 2013).

2.2. Magnitude of Issue

The Office of Personnel and Management (OPM) is responsible for the conduct of background investigations for prospective and current employees across the government. Every security clearance is tracked by this organization. A *2013 Report on Security Clearances Determinations* published by the Office of the Director of National Intelligence states that as of October 1, 2013 there were 3,091,977 individuals eligible for access to classified

© 2014 The SANS Institute Author retains full rights.

information. This is a substantial quantity of potential targets for identify thief and/or more lucrative leveraging of clearance information.

To make matters worse, the amount of personal information collected is staggering. The Questionnaire for National Security Position Standard Form 86 dated December 2010 is 127 pages of information required by an applicant (Form 86, 2010). Included is this form is all the information about the individual, their family, their education, their work experience, military experience, criminal information, and additional information about everyone in their family. It is certainly enough information aggregated in one location to ensure that someone can easily compromise that information and potential any family member's identity.

3. How to Fix It!

3.1. Critical Security Controls

Critical Security Control 17: Data Protection is the key control that would have prevented or minimized this compromise. "The phrase Data Loss Prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data is use (e.g. , endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with centralized management framework" (Tarala, Cole, 2014, p. 1-35). This control is best achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques.

The OPM relied on defense-in-depth to protect the sensitive information and over time the failure of one or more controls lead to the loss of this information. Verizon data shows that hacking and malware categories if exploitation exploded upward in 2009 with substantial increases again in 2013 data (Verizon, 2014). A mixture of the fifteen suggestions provided by SANS for implementing the Data Protection Controls would have provided a

© 2014 The SANS Institute Author retains full rights.

final secure last layer that after all other defense-in-depth controls failed would have rendered the attack useless.

Several key areas of the Critical Security Control 17 that would have invalidated this data breach include: (CSC 17-1) deploy encryption on mobile devices and systems that hold sensitive information; (CSC 17-2) ensuring encryption uses vetted algorithms; (CSC 17-3) perform an assessment to identify sensitive information; (CSC 17-7) employ encryption when moving data; and (CSC 17-11) perform an annual review of algorithms. Implementing cryptography provides confidentiality, integrity, authentications, and non-repudiation and provide a final defense against theft.

3.1.1. CSC 17-1 – Encryption at Rest

Both Oracle and Microsoft employ a technology titled Transport Data Encryption (TDE). This file level encryption goes a long towards protecting the data at rest by encrypting the information on the hard drive which solves the backup media issues by ensuring the data that is backed up is encrypted.

Microsoft provides TDE in Microsoft SQL Server 2008 Enterprise edition and later. It is not available in the Business Intelligence, Standard, or Express editions. The implementation is completely transparent to the applications requiring no coding changes. (Otey, 2013).

Oracle's provision of TDE requires the Advanced Security Options in Oracle 10g and later. Oracle provides two controls in this space to include data at rest and redaction of sensitive data displayed by applications (Oracle Database, 2013).

Ramdas Kenjael of TransUnion states, "We were able to encrypt the data and become compliant within a matter of weeks." (Bottger, 2012). Mr. Bottger identifies that no application changes are required, performance impact is +/- 1%, there will be no deployment

© 2014 The SANS Institute Author retains full rights.

downtime, and the implementation works seamlessly with partitioning and compression.

Ensuring key information is managed in a fashion that provides a level of encryption commensurate with the value of the information provides a defense-in-depth control that is the last barrier to protecting the confidentiality of information.

3.1.2. CSC 17-2 – Vetted Algorithms

"Kerckhoffs's principle was stated by Auguste Kerckhoffs in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge" (Wikipedia, Kerckhoffs's principle). The National Institute of Standards and Technology provides guidance to ensure that encryption algorithms are well vetted and are based on solid algorithms. Currently the three approved encryption algorithms are AES, Triple DES, and Skipjack (NIST, 2014).

Security through obscurity is not security. The use of well vetted encryption algorithms ensure that the enterprise is secure in the knowledge that the best options available have been applied. Even if the enterprise is not mandated by regulations, the use of NIST approved encryption is an excellent way to ensure the selected encryption is worth the investment.. As stated in SANS 512, "Perhaps the most important lesson in this chapter is that ciphers should be developed in the open, taking advantage of the collective brainpower of cryptologists throughout the world. This kind of scrutiny and reliance on proven technology reduces the likelihood that a weak algorithm is used, and encourages cipher designers to place all of the cryptosystem's security in the key rather than the algorithm itself." (SANS, 2011. p. 78). Using NIST approved algorithms ensure this is the case.

© 2014 The SANS Institute Author retains full rights.

3.1.3. CSC 17-3 - Identify Sensitive Information

The National Institute of Standards and Technology (NIST) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* provides the following recommendations; 1) identify all PII in the environment; 2) minimize the use, collection, and retention to what is necessary; 3) categorize based on confidentiality impact level; 4) apply the appropriate safeguards based on impact level; and 5) develop an incident response plan to handle breaches. (McCallister, E., Grance, T., Scarfone, K. ,2010).

To protect the enterprise from compromise and ligation, it is incumbent on the enterprise to reduce collection, understand its use, and understand where it resides in the enterprise. If controls are not in place to prevent propagation of the information outside of central repositories, the enterprise will not be able to understand what has been stolen when a compromise happens. This will substantially increase the liability of the enterprise.

3.1.4. CSC 17-7 – Encryption in Motion

The use of network tunnels provide legitimate opportunities to aggregate traffic, leverage protocols to create more effective communications channels and to provide confidentiality. There are a few published secure protocol standards such as Internet Protocol Security (IPsec), Secure Socket Layer (SSL), and Transport Layer Security (TLS). The standards are designed to provide end-to-end encryption of traffic regardless of route. (Davidoff, 2012, p. 427).

TLS use has become quite popular on the Internet as a VPN tunneling protocol. This Internet Engineering Task Force Standard was designed to provide secure communications across the Internet.

At the OPM, the E-QIP system is a web based interface to a database. Implementing TLS provides confidentiality and integrity of

© 2014 The SANS Institute Author retains full rights.

information in motion between the requester and the server. This is the most popular approach to implementing public-key encryption. Every browser today is configured with this capability using certificates from trusted certificate authorities.

Implementing this capability provides a secure environment for data in motion. To break this secure communications capability, the attacker would be required to capture traffic that includes the TLS/SSL handshake and subsequent traffic between the requester and server. The attacker could then use the server's private key to recover the session keys and decrypt the contents. According to Davidoff, this attack only works with RSA key exchanges. The Diffie-Hellman key exchange is not vulnerable to this attack (Davidoff, 2012, p. 397)

Another approach would be to route traffic through an attacker's proxy server. This would require the attacker have control of the requesting system to route the traffic to the proxy server that is controlled. A simple solution to this compromise that attempts to use an inside computer is to ensure that Source Routing is disabled within the enterprise's network. In addition, the victim will get warnings about the potential man in the middle attack while initiating the session as part of the web session initiation. Unfortunately, many people ignore these warnings in today's environment (Davidoff, 2012, p. 396).

The SHA-1 algorithm has been identified as potentially insecure. This hashing function has been used with SSL since the 1990s. The GoDaddy Support site recommends the immediate re-key of SSL certificates to support SHA-2 hash capability (GoDaddy, 2014). The site suggest that Microsoft is driving this change and that soon Google will begin issuing warnings about security issues from within their Chrome browser for all visitors using SHA-1 this year. With the

© 2014 The SANS Institute Author retains full rights.

deprecation of SHA-1 and its replacement with SHA-2, encrypting data in motion will ensure additional protection for critical information.

3.1.5. CSC 17-11 – Annual Review of Encryption

This control is only as good as the application of the previous controls. As the information protection requirements changes, new technology is implemented and/or the implementation of the encryption infrastructure is modified; it is prudent to review all facets of the encryption. While changes to algorithm might be rare, the implementation and technology are potentially very dynamic. Proper implementation of the technology is a requirement to ensure the benefits of this final defense-in-depth control.

4. Conclusion

Many attempts have been made at legislating the issues surrounding PII. The failures and subsequent compromises of this sensitive information continue to escalate. Legislation alone will not solve this problem.

Several companies have made substantial effort to quantify the losses of information and the methods of attack (Ponemon, Verizon). The cost of a breach continues to increase while the security environment becomes more and more complex. The adversary skill sets are rapidly improving and the tool set to assist them is escalating in capability

The NYT article entitled "*Chinese Hackers Pursue Key Data on U.S. Workers*" (Schmidt, 2014) provides yet another account of the loss of sensitive information. Recently the US Investigative Services (a subcontractor to OPM) was advised their contract would not be renewed after the recent breach of their systems. Nick Wakeman proposes that this announcement should scare all of us. First the backlog on clearance investigations will be slowed down substantially. In addition, normally the Federal government has worked with affected subcontractors to remedy the problem. With this

© 2014 The SANS Institute Author retains full rights.

termination of the contract, will there be incentives for companies to not self-report? (Wakeman, 2014).

National State attacks are becoming more and more dramatic and the success rate is phenomenal. Information relating to the identities of over 3 Million people who have access to National Secrets has been compromised. Certainly there are concerns over Identify Theft, but a bigger issue is how the Nation State will pursue this information to further country's mission.

Critical Security Control 17: Data Protection is the key control that would have prevented or minimized this compromise. This control is best achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques (Tarala, Cole, 2014). The OPM was relying on defense-in-depth to protect the sensitive information and over time industry will learn of multiple failures that lead to the loss of this information. A mixture of the 15 suggestions for implementing the controls would have provided a final secure layer that after all other defense-in-depth controls failed would have rendered the attack useless.

Controls fail! The concept of defense-in-depth is designed to provide additional layers of protection to accommodate these failures. The proper implementation of Critical Control 17 would render all other failures invalid as the perpetrator would only steal information that could not be used. When this control is applied properly, sensitive information would be secure as required by the Organization for Economic Co-operation and Development (OECD). The OECD provides 8 privacy principles. Principle 5: Security Safeguards, advises that information must be protected by reasonable safeguards (SANS, 2011. p. 218). Control 17 would have provided the final security safeguard to preventing a compromise of the enterprise from becoming a data breach. The cost of mitigating a data breach is expensive, time consuming, and damaging to the enterprise's reputation.

Revelations from the Snowden event provides clear evidence that the fundamental math behind good encryption is still solid. Cryptography experts told the MIT Technology Review staff that after the experts performed a review of relevant material that thy believe the Nationals Security Administration had not crack the underlying

© 2014 The SANS Institute Author retains full rights.

mathematical operations. (Simonite, 2013). Concern is not the encryption and basic math but attacks against the humans and organizations that use the encryption. While there are methods that supposedly enable cracking the good encryption, these methods require the ability to listen to the sounds generated by the computer's CPU as the decryption is occurring. This would require have physical access minimizing this risk (Anthony, 2013).

According to urban legend, the famous gangster, Willie Sutton, once said he robbed banks because that's where the money is. Why would someone break into the OPM? It is because that is where the sensitive information relating to people who have access to our country's most sensitive information resides. At the very least OPM should have implemented a defense-in-depth strategy that included Critical Control 17 to protect the information that was entrusted to OPM's care. This breach of information will have impacts for years to come. A solid implementation of Critical Security Control 17: Data Loss Protection would have rendered the breach invalid.

5. References

Anthony, S. (2013, December). Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU. *Extreme Tech*. Retrieved from http://www.extremetech.com/extreme/173108-researchers-crack-the-worlds-toughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu

Bottger, T. (2012). Oracle Database 12c. *Oracle Advanced Security Transparent Data Encryption.*

Conrad, E., Misenar, S., Feldman, J. (2012). Domain 5: Cryptography. *CISSP Study Guide 2E* (pp. 213-255). Waltham, Massachusetts: Syngress.

Davidoff, S., Ham, J. (2012). Network Tunneling,, *Network Forensics Tracking Hackers Through Cyberspace* (pp. 423-440). Upper Saddle River, New Jersey: Prentice Hall.

GoDaddy Support (2014). *Information About Requiring the SHA-2 Hash Function*. Retrieved from http://support.godaddy.com/help/article/4818/information-about-requiring-the-sha-2-hash-function

Herrmann. D. (2007). Personal Privacy. *Complete Guide to Security and Privacy Metrics*. Boca Raton, Florida: Auerbach Publications.

McCallister, E., Grance, T., Scarfone, K. (2010). National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (Special Publication 800-122).

David W. Belangia, dwbelangia@hotmail.com

© 2014 The SANS Institute Author retains full rights.

(NIST) National Institute of Standards and Technology, Cryptographic Toolkit, Approved Algorithms. Retrieved from http://www.csrc.nist.gov/groups.ST/toolkit/block-ciphers.html.

Office of the Director of National Intelligence. (2013). *2013 Report on Security Clearance Determinations.* Retrieved from http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1051-2013-report-on-security-clearance-determinations

Oracle Database 12c. (2013). *Encryption and Redaction in Oracle Database 12c with Oracle Advanced Security.*

Otey, M. (2013). SQL Server Pro *SQL Server Encryption Options*. Retrieved from http://sqlmag.com/database-security/sql-server-encryption-options.

Ponemon Institute Research Report. (2014). *2014 Cost of Data Breach Study: Global Analysis*. Retrieved from http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Questionnaire for National Security Position Standard/Form 86, 5 CFR Parts 731, 732, an 736. (2010).

SANS Institute. (2011). *Management 512.3 Secure Communications.* (p. 78)

Schmidt, M., Sanger, D., Perlroth, N. (2014, July). Chinese Hackers Pursue Key Data on U. S. Workers. *The New York Times.* Retrieved from http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0

Simonite, T. (2013, September). NSA Leak Leaves Crypto-Math Intact but Highlights Known Workarounds. *MIT Technology Review*. Retrieved from http://www.technologyreview.com/news/519171/nsa-leak-leaves-crypto-math-intact-but-highlights-known-workarounds

Tarala, J., Cole, E. (2014). Overview of Critical Control 17, *Audit/Security 566 Implementing and Auditing the Critical Security Controls-In-Depth, Book 5*, (pp. 35-66). SANS Institute.

U.S. Department of Energy. (2013). *July 2013 Cyber Incident.* Retrieved from http://energy.gov/cio/cyber-incident-information/july-2013-cyber-incident

Verizon. (2014). *2014 Data Breach Investigation Report*. Retrieved from http://www.verizonenterprise.com/DBIR/2014/

Wakeman, N. (2014, September). Why the fall of USIS should scare the rest of us. *WT Business Beat*. Retrieved from http://washingtontechnology.com/editors-notebook/2014/09/usis-contract-cancellation.aspx?s=wtdaily_110914&m=2

Consensus Audit Guidelines. Retrieved from http://www.sans.org/critical-security-controls/

Wikipedia, Kerckhoffs's principle.

David W. Belangia, dwbelangia@hotmail.com

© 2014 The SANS Institute Author retains full rights.