LESSONS LEARNED

Office of Personnel Management Breach

With the breach at the Office of Personnel Management (OPM), the U.S. government suffered the biggest cybersecurity failure in history.

In April, the OPM discovered personal data from 4.2 million current and former Federal government employees had been stolen. Experts from the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI) and the OPM formed a multiagency team of investigators and determined that the initial discovery was only the tip of a very chilling iceberg.

After several weeks, the OPM reported on its website, "OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."[1]

bsi.

...making excellence a habit.™

According to an article by Eric Chabrow in GovInfoSecurity, Mark Weatherford, the former deputy undersecretary for cybersecurity at the Department of Homeland Security, indicated the OPM failed to implement some very basic security controls. After the fact, the OPM implemented additional network security precautions, including installing anti-malware software, limiting remote access for network administrators and restricting remote network administration functions. But according to Weatherford "This is jacks or better to open; if you're not already doing this stuff, you're not even at the game."[2]

Quoting an interview with Information Security Media Group, the article went on with Weatherford noting that while the precautions may not have completely stopped the attack, they would have made it a lot more difficult. He summarized it by saying "If they're not deploying anti-malware in their systems already, come on, this is kindergarten stuff."[3] The OPM is just the latest in cybersecurity-related problems. According to the Government Accountability Office, "Federal agencies have significant weaknesses in information security controls that continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support their operations, assets, and personnel. For example, in their performance and accountability reports and annual financial reports for fiscal year 2014, 17 of 24 major federal agencies indicated that inadequate information security controls were either material weaknesses or significant deficiencies."[4] While this only represents known exposures, it clearly demonstrates the significant vulnerabilities in the government's cybersecurity policies.

No intrusion detection and prevention system is infallible, however, as they can only address known threats. In an interview with InfoRisk Today, Gartner expert Claudio Neiva says "there is only so much an intrusion detection and prevention system can do."[5] Unknown threats can only be stopped by improving the way you execute processes and also by enforcing security policy with employees. Organizations need to take additional steps to safeguard critical data and systems.

The OPM had been warned repeatedly that its cybersecurity systems were poor. In a 2010 report, the OPM's Office of Inspector General stated, "We continue to consider the IT security management structure, insufficient staff, and the lack of policies and procedures to be a material weakness in OPM's IT security program."[6]

In questioning OPM Director Katherine Archuleta in the June 25, 2015 hearing, House Oversight Chairman Jason Chaffetz (R-UT), maintained that "The Inspector General [in] November 12, 2014 [stated] we recommend that the OPM Director consider shutting down information systems that do not have current and valid authorization."[7] Chaffetz also criticized the OPM for its inability and unwillingness to address security flaws that had been repeatedly identified in Inspector General reports dating back to 2007.

In looking at the facts of the case and pulling from various quotes above, we can explore how this incident may have been avoided or its impact minimized if a verifiable management system standard, such as ISO/IEC 27001 for an Information Security Management System (ISMS), was in place.

---

[1] https://www.opm.gov/cybersecurity/ Accessed 7/20/2015.

[2] Eric Chabrow. Dissecting the OPM Breach, GovInfoSecurity, June 5, 2015 http://www.govinfosecurity.com/interviews/dissecting-opm-breach-i-2732?rf=2015-06-08-eg&mkt_tok=3RkMMJWWfF9wsRokuq%2FNZKXonjHpfsX57ewtWqSg38431UFwdcjKPmjr1YEATcV0aPyQAgobGp5I5FEIT7HYRrhpt6cOXA%3D%3D#. Accessed 7/20/2015.

[3] Ibid.

[4] http://www.gao.gov/key_issues/cybersecurity/issue_summary, Accessed 7/20/2015.

[5] Eric Chabrow, Why Detection Systems Don't Always Work, June 10, 2015 http://securityintelligence.inforisktoday.com/interviews/detection-systems-dont-always-work-i-2741 Accessed 7/20/2015.

[6] https://oversight.house.gov/wp-content/uploads/2015/06/FY2010-OPM-IG-excerpt.pdf.

[7] http://www.c-span.org/video/?106792-1/radio-office-personnel-management-data-breach.

According to Mark Weatherford, the former deputy undersecretary for cybersecurity at the Department of Homeland Security, the OPM failed to implement some very basic security controls. "This is jacks or better to open; if you're not already doing this stuff, you're not even at the game."

In ISO/IEC 27001:2013 Sections 4 – 10 outline all the requirements for a holistic ISMS structure of an organization related to:

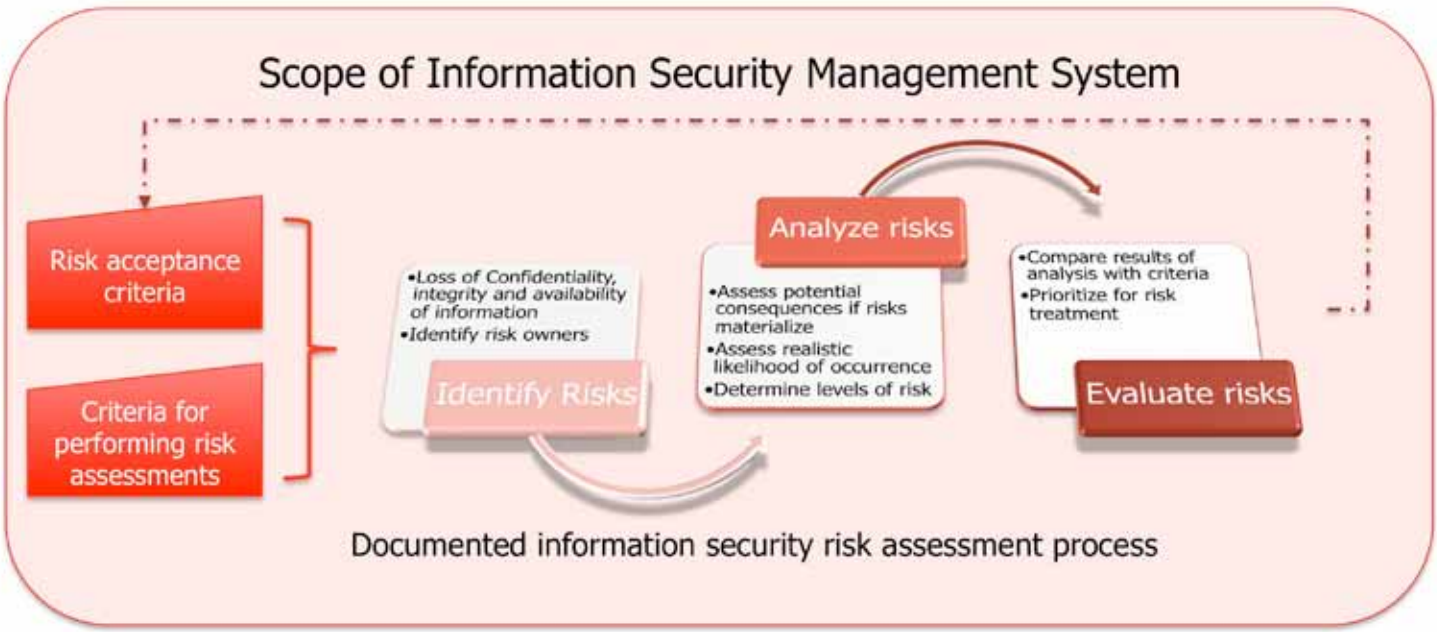
4. Context of the organization
5. Leadership
6. Planning
7. Support
8 Operation
9. Performance evaluation
10. Improvement

Initially, the two main areas of focus should be on Leadership and Risk as depicted by the following graphs:

Figure 1 - 5.1 Leadership and commitment

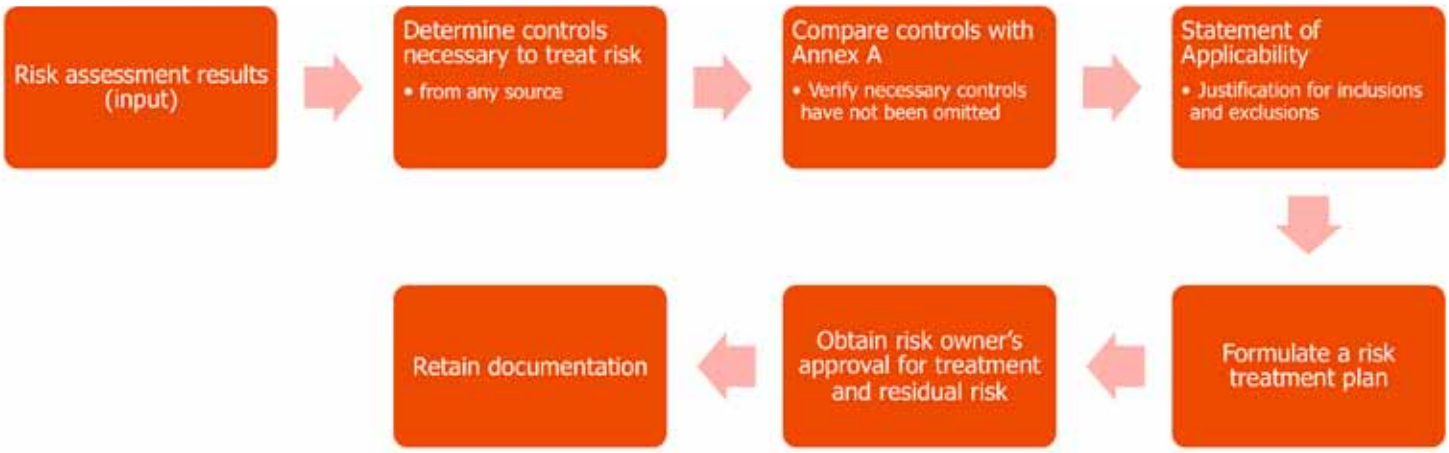
Source: Kiyoshi Kataoka ISMS global scheme manager for BSI

Figure 2 – Risk Assessment in Information Security Management System



Source: Robert Whitcher ISMS scheme manager for BSI

Figure 2 - 6.1.3 Information Security Risk Treatment



Source: Kiyoshi Kataoka ISMS global scheme manager for BSI

After the fact, OPM implemented additional network security precautions, including installing anti-malware software, limiting remote access for network administrators and restricting remote network administration functions.

The following specific controls in ISO/IEC 27001:2013's Annex A address these areas[8]:

A.12.2 Protection from malware with the objective to ensure the information and facilities are suitably secure.

A.12.2.1 Controls against malware includes the controls that detect, prevent and recover information combined with user awareness/ competency.

A.13.1 Network security management with the objective to protect information networks and processing centers.

A.14.1 Security requirements of information systems includes controls to provide information security at every touchpoint in an organization as well as those systems that provide services over public networks.

In an interview with InfoRisk Today, Gartner expert Claudio Neiva says there is only so much an intrusion detection and prevention system can do. Unknown threats can only be stopped by improving the way you execute processes and also by enforcing security policy with employees. Organizations need to take additional steps to safeguard critical data and systems.

The following sections of ISO/IEC 27001:2013, paraphrased below, could be directed to these areas:

5.1 Leadership and commitment
Top management shall demonstrate leadership and commitment with respect to the information security management system developing an ISMS policy in line with organization's strategic direction, committing the resources required to institute the policy, communicating it across the organization, testing its effectiveness and ensuring it integration throughout the organization's processes.

[8] International Standard ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements, Annex A, Reference control objectives and controls, second edition 2013-10-1.

5.2 Policy
Top management shall establish an information security policy that is appropriate, provides the framework for setting information security objectives, clearly demonstrates a commitment to information security and its continual improvement, is documented, communicated and readily available.

7.3 Awareness
Workers under the organization's control shall be made aware of the ISMS policy, their role in its effectiveness and the consequences of not following the policy:

7.4 Communication
The organization shall determine the need, methodology, processes and responsible person for internal and external communications relevant to the information security management system including:

In questioning OMP Director Katherine Archuleta in the June 25, 2015 hearing, House Oversight Chairman Jason Chaffetz (R-UT), maintained that "The Inspector General [in] November 12, 2014 [stated] we recommend that the OPM Director consider shutting down information system that do not have current and valid authorization." Chaffetz also criticized the OPM for its inability and unwillingness to address security flaws that had been repeatedly identified in Inspector General reports dating back to 2007.

9.2 Internal audit
The organization shall conduct internal audits at planned intervals to determine if the ISMS is effectively implemented and maintain to meet the requirements of the organization and the standard as well as develop an effective audit program. In this regard

9.3 Management review
Top management shall review the organization's ISMS at regular, pre-determined intervals to ensure its applicability and effectiveness.

10.1 Nonconformity and corrective action
When the ISMS falls out of conformity, the organization shall take the necessary action to correct the problem as well as handle any fallout the nonconformity caused, and ensure steps have been taken to reduce the likelihood of a reoccurrence, including an corrective action plan, which will be properly documented and retained.

About BSI

BSI provides training, assessment and certification, and software solutions to protect your organization. As an Information Security Management System, ISO/IEC 27001 is designed to help you select adequate and well-balanced security controls, which will protect information assets and give confidence to interested parties, including your customers. Certification to ISO/IEC 27001 is an essential safeguard for any organization.

BSI's range of training courses are designed to provide the tools you and your staff need to understand ISO/IEC 27001, as well as oversee audit programs for your management system. BSI works with this standard, and many more, to protect your organization's most valued assets, including the relationship between you and your customers, from potential threats

Bibliography

Chabrow, E. (2015, June 5). Dissecting the OPM Breach. *Goverment Infosecurity*. Retrieved from http://www.govinfosecurity.com/interviews/dissecting-opm-breach-i-2732?rf=2015-06-08-eg&mkt_tok=3RkMMJWWfF9wsRokuq%2FNZKXonjHpfsX57ewtWqSg38431UFwdcjKPmjr1YEATcV0aPyQAgobGp5I5FEIT7HYRrhpt6cOXA%3D%3D

Chabrow, E. (2015, June 10). Why Detection Systems Don't Always Work. *infoRisk Today*. Retrieved from http://www.inforisktoday.com/interviews/detection-systems-dont-always-work-i-2741?rf=2015-06-12-eh&mkt_tok=3RkMMJWWfF9wsRokua3AZKXonjHpfsX57ewtWqSg38431UFwdcjKPmjr1YEFTcd0aPyQAgobGp5I5FEIT7HYRrhpt6cOXA%3D%3D

Chaffetz, Jason, "House Oversight Committee Hearing." C-Span video. June 25, 2015. http://www.c-span.org/video/?106792-1/radio-office-personnel-management-data-breach

"Federal Information Security Manggement Act Audit FY2010 Report 4A-CI-00-10-019."*U.S. Office of Personnel Management Office of the Inspector General."* https://oversight.house.gov/wp-content/uploads/2015/06/FY2010-OPM-IG-excerpt.pdf

International Organization for Standardization, ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements, Annex A, Reference control objectives and controls, second edition 2013-10-1.

Office of Personnel Management, Cybersecurity. https://www.opm.gov/cybersecurity.

Schwartz, M. J. (2015, June 15). Millions More Affected by OPM Breach. *BankInfo Security*. Retrieved from http://www.bankinfosecurity.com/millons-more-affected-by-opm-breach-a-8311?rf=2015-06-15-eb&mkt_tok=3RkMMJWWfF9wsRokua%2FNZKXonjHpfsX57ewtWqSg38431UFwdcjKPmjr1YEFTsB0aPyQAgobGp5I5FEIT7HYRrhpt6cOXA%3D%3D

U.S. Government Accounting Office. *Key Issues.Cybersecurity* available . http://www.gao.gov/key_issues/cybersecurity/issue_summary

bsi.

For information on Lessons Learned regarding other cybersecurity breaches, visit our website on www.bsiamerica.com

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA

Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
Web: www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada

Tel: 1 800 862 6752
Fax: 1 416 620 9911
Email: Inquiry.canada@bsigroup.com
Web: www.bsigroup.ca
www.bsigroup.ca/fr

BSI/USA/472/MS/0715/E