CS-465/565 Information Assurance Project

Dr. Chuck Cartledge

23 January 2107

Contents

1 Introduction

> *"Information assurance is ensuring that your information is where you want it, when you want it, in the condition that you need it and available to those that want to have access to it – but only them."*
>
> Blyth and Kovacich [1]

There was a major data breach in recent months reported in the news. Here are some of the I'net articles that were written (there are hundreds more):

- August 13, 2016, *Security News This Week: The DNC Hack Was Worse Than We Thought* [1]
- December 12, 2016, *Did the Russians hack the election? A look at the established facts* [2]
- December 12, 2016, *How we know Russia, not a guy in Jersey, hacked the DNC* [3]
- December 13, 2016, *Heres The Evidence Russia Hacked The Democratic National Committee* [4]
- December 14, 2016, *Heres the Public Evidence Russia Hacked the DNC Its Not Enough* [5]
- December 14, 2016, *Top Democrat's emails hacked by Russia after aide made typo, investigation finds* [6]

[1] https://www.wired.com/2016/08/security-news-week-dnc-hack-worse-thought/
[2] http://arstechnica.com/security/2016/12/the-public-evidence-behind-claims-russia-hacked-for-trump/
[3] http://thehill.com/blogs/pundits-blog/technology/309956-how-we-know-russia-not-a-guy-in-jersey-hacked-the-dnc
[4] http://time.com/4600177/election-hack-russia-hillary-clinton-donald-trump/
[5] https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/
[6] https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds

- December 15, 2016, *DNC docs were leaked, not hacked, intelligence veterans say* [7]
- December 20, 2016, *How We Identified the D.N.C. Hacks 'Patient Zero'* [8]
- January 3, 2017, *The Download on the DNC Hack* [9]

These data breaches resulted in unauthorized personnel gaining access to restricted data, other breaches prevented authorized personnel from accessing necessary data.

2 Assignment

Your assignment is to take on the role of Chief Information Assurance Officer (CIAO) for the **DNC**. As part of that role, you are to:

1. Conduct a postmortem on the event and identify as many root causes as practical (you can exercise a certain amount of create license in this topic),
2. Recommend sanctions or instructive actions for the people involved,
3. Identify specific corrective actions for people, processes, and procedures to help ensure that a similar type of data breach does not occur in the future.

Be sure to couch your recommendations using the risk management ideas from chapters 3 and 11 of the text.

3 Deliverable

A PDF report meeting the following physical and logical requirements:

1. Between 10 - 15 pages (not including front matter, back matter, or figures from other sources). Front matter includes things like title page, table of contents, list of tables, list of figures, etc. Back matter includes things like references or appendices.
2. If you include tables or figures, then they must be referenced in the text. Remember that tables and figures need captions, and that the captions show up in the front matter. Captions can be as long or large as necessary, but large captions should not show up in the table of contents. (For those of with a LaTeX bend, you might want to check out the optional argument to the caption macro.)
3. Use your word or text processor to create the front and back matter. It is easy to tell when someone has tried to do it by hand, so please don't.
4. You can use whatever resources you feel are appropriate, just be sure to cite them.
5. Spell check, spell check, and then spell check again.
6. If your word or text processor does not save files natively as PDFs (meaning that you have to "export", or "print" them), be sure and look at the file in an external reader (Adobe Acrobat is probably the best). Not all browsers implement all aspects of the PDF specification, so check your product with a real reader to see what it looks like.

[7] `https://www.rt.com/usa/370447-russia-hack-intelligence-dissent/`
[8] `https://www.nytimes.com/2016/12/20/insider/how-we-identified-the-dnc-hacks-patient-zero.html?_r=0`
[9] `https://krebsonsecurity.com/2017/01/the-download-on-the-dnc-hack/`

7. Be sure to address each of the line items identified in the Assignment section, and make it easy for me to find them. A suggestion is to have each item be a section or chapter that stands proud in the Table of Contents.

References

[1] Gerald Kovacich Andrew Blyth, *Information assurance, security in the information environment*, 2006.