William F. Slater, III

M.S. in Cybersecurity Program

Bellevue University, Bellevue, NE

Information Security Management - (CIS 608)

August 29 – November 19, 2011

Instructor: Professor Gary Sparks

Week 03, Assignment 3.1

Due Sunday, September 18, 2011, 23:59 Central Time

Submitted Sunday, September 18, 2011, 22:00 Central Time

Assignment Description:

This assignment is worth 50 points.

Read through the Data Breach Report links above. This might take a little while, and you may want to make notes to yourself while reading. Look at the data for all three years and provide a summary of at least five major trends identified over the last three years. Include in your posting your opinion regarding at least 3 of the trends. For example, did the number of viruses rise? Fall? Why?

You still need outside references, so you may want to investigate and determine whether the stated trends are reported by others, or provide more information on those trends.

Brief Analysis of Data Breach Trends, 2008 - 2010

William Slater

CIS 608 Information Security Management

Bellevue University

Week 3, Assignment 3-3

Gary Sparks, M.S. - Instructor

September 18, 2011

Introduction

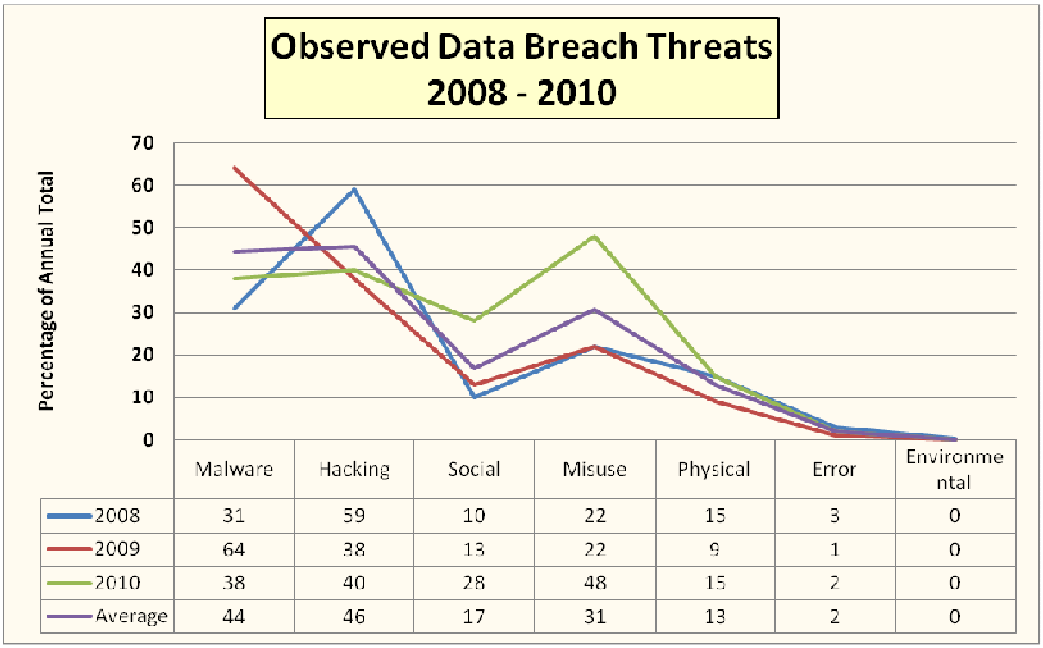
This paper contains a brief trend analysis of data and statistics about data breaches from three separate annual reports whose primary focus were the analysis of data breaches. Members of the Verizon Business Risk Team did the research and compiled these reports using over 500 investigations and 10s of thousands of data points for each report. The broad spectrum of types of companies and data points collected provides increased credibility making this annual data breach report one of the most authoritative in the world of Information Security. In addition, the trends shown in these annual data breach reports can be used by other management teams to help formulate the security plans, strategies, and budgets that will mitigate the risks that these threats and actual data breach methods represent.

Threat Action Category Trends

The table and accompany graph below show the categories of Threat Actions and the percent increases in each year from the previous year for each category. Notice that the top threats are Malware, Hacking, Social Engineering and Misuse.

Threats Actions				
Category	2008	2009	2010	Average
Malware	31	64	38	44
Hacking	59	38	40	46
Social	10	13	28	17
Misuse	22	22	48	31
Physical	15	9	15	13
Error	3	1	2	2
Environmental	0	0	0	0

(Baker, 2009, 2010, 2011)



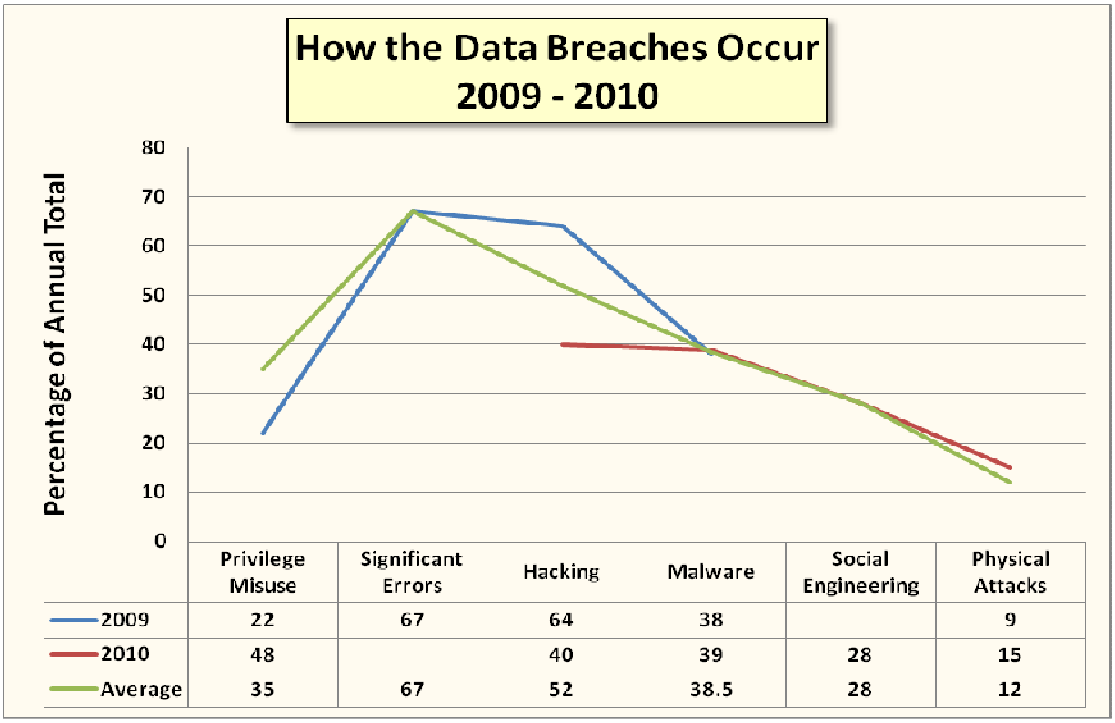
(Baker, 2009, 2010, 2011)

The Source of the Data Breaches

The table and accompanying graph below show the categories of the Source of Breaches and the percent increases in each year from the previous year for each category. Note that the biggest causes of data breaches were Significant Errors, Hacking, Malware, and Privilege Misuse. Also note that uniformly categorized and summarized data was not available for 2008.

How Do Data Breaches Occur?				
Category		2009	2010	Average
Privilege Misuse		22	48	35
Significant Errors		67		67
Hacking		64	40	52
Malware		38	39	38.5
Social Engineering			28	28
Physical Attacks		9	15	12

(Baker, 2010, 2011)



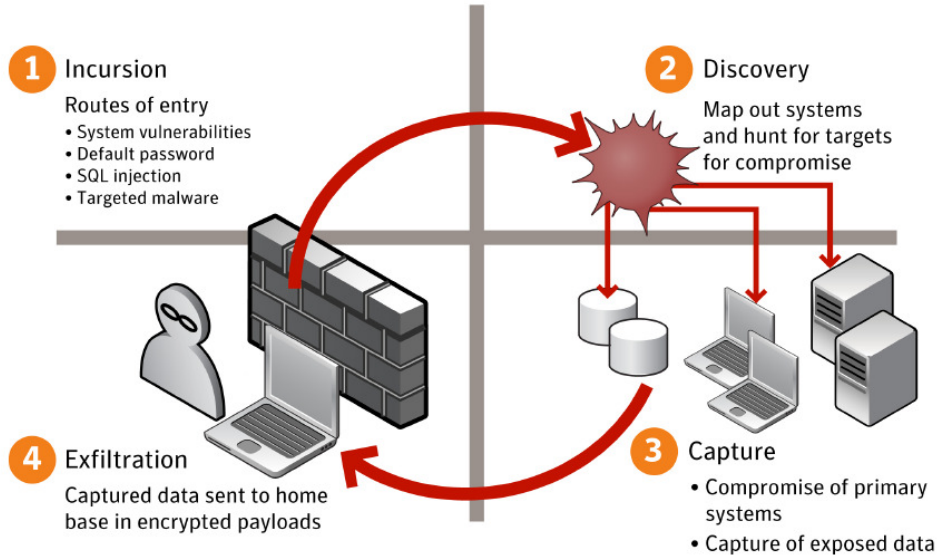
	Privilege Misuse	Significant Errors	Hacking	Malware	Social Engineering	Physical Attacks
2009	22	67	64	38		9
2010	48		40	39	28	15
Average	35	67	52	38.5	28	12

(Baker, 2010, 2011)

Additional Useful Information

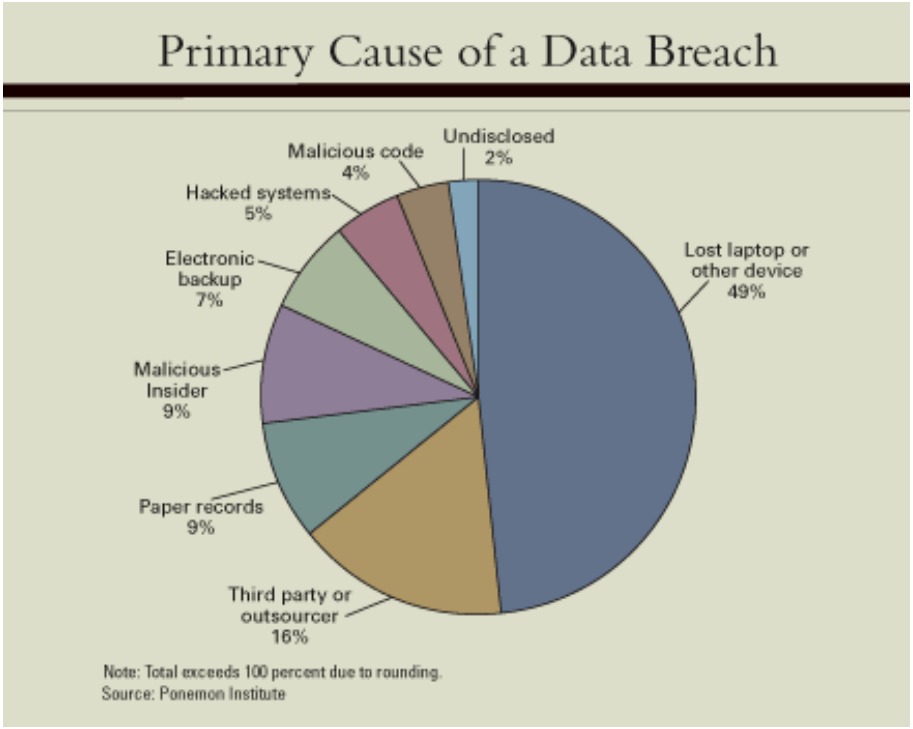
As required by the assignment description, I consulted additional resources regarding data breaches and threats that are inherent in the modern networked computer environment. The diagrams and information below are the results of this research.

The diagram below from a Symantec whitepaper shows at a high level the four phases of a targeted attack. After careful review of this, it occurred to me, based on my knowledge of penetration testing for purposes of certification and accreditation, that there is at least two missing phases that should be part of the attack: 1) the reconnaissance phase where the information required for the attack is gathered; and the 2) characterization / planning phase, where the data collected from the reconnaissance phase is analyzed and structured into a plan.



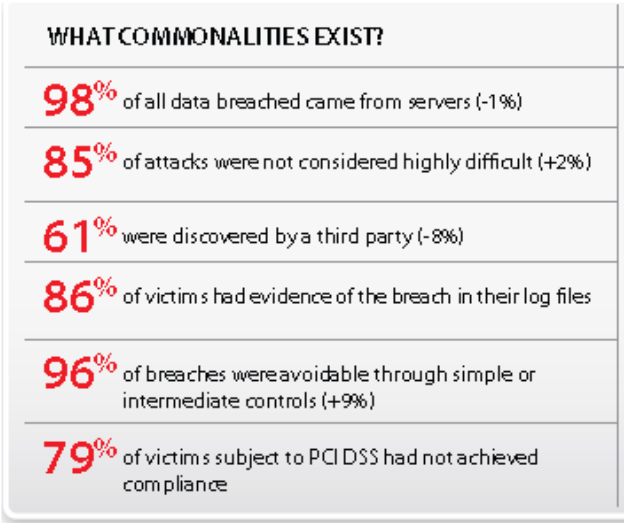
Four Phases of Targeted Attacks
(Symantec, 2009)

The Ponemon Group produced a similar study of data breaches in 2009. That data is summarized by causes of data breaches in the chart shown below. Again, this highlights the need for Information Security Managers to understand these risks and how to effectively plan mitigate them.



(Ponemon Institute, 2009)

The diagrams below show the commonalities in the data breaches that occurred in 2010:

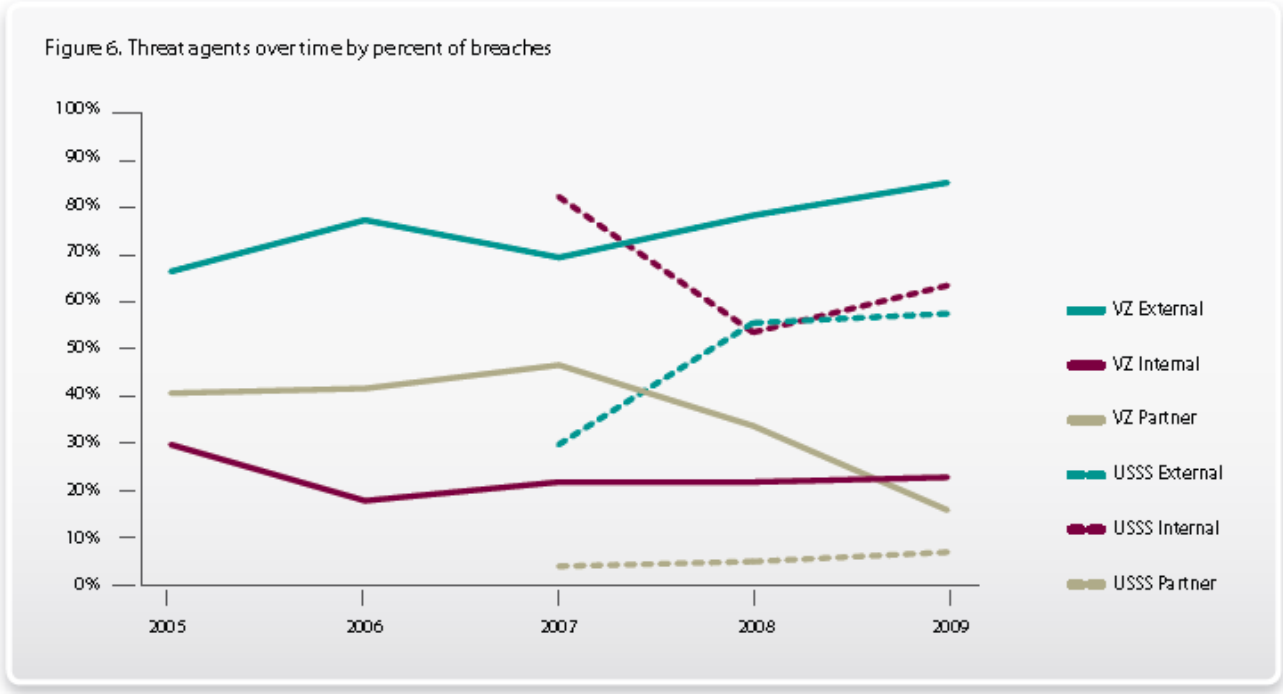


(Baker, et al, 2010)

Based on the data breach analysis study in 2010, the diagram below shows the recommendations on how to plan mitigation efforts:

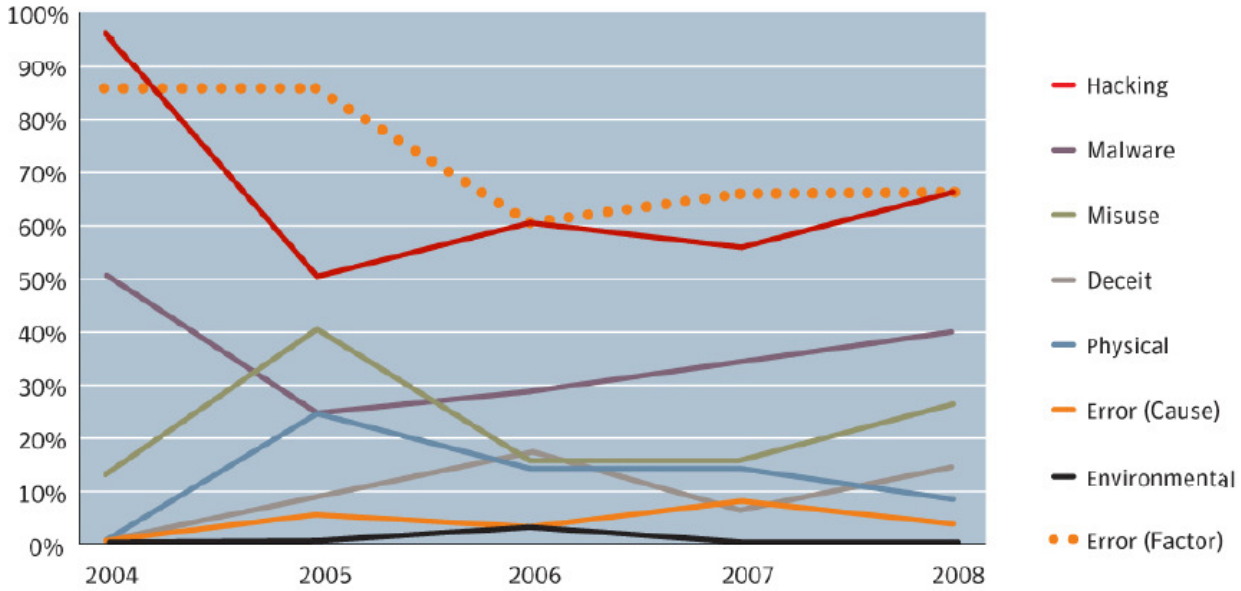
(Baker, et al, 2010)

The chart below shows the data breach threat agent trends by percentage of breaches over the past several years. What this chart shows is that external threats have been steadily increasing since 2005.



(Baker, et al, 2010)

The diagram below showing the 2004 – 2008 trends of data breach causes was provided in a Symantec white paper, but the original source was Baker's 2009 Verizon Data Breach Analysis study:



(Symantec, 2009)

Conclusion

The general conclusions that a manager can draw from these reports are as follows:

1) The increases in Threat Actions over the past three years have been the areas of

   Hacking

   Social Engineering

   Malware Attacks

2) The external threats have been steadily increasing in most companies since 2005.

3) Knowing where these threats are coming from and how these data breaches are occurring will help the prudent manager create a plan and a road map for the expenditure of the resources to mitigate these risks as effectively as possible.

4) The general need for Information Security personnel to carry out these hands-n mitigation activities is increasing, so we can expect a growth of professionals with these specialized skills in our IT staffs.
5) Because of the increased focus on publicity about data breaches as well as compliance with laws that are designed to protect consumer privacy, every manager must make the protection of the data of its clients and its employees a top priority, and secure budgets that will fund the necessary resources to protect data and drive down the risks to a level that is acceptable for the business to effectively operate in compliance with all existing laws.

References:

Baker, W. H., et al. (2009). 2008 Data Breach Investigations Report: A Study Conducted by the Verizon Business Risk Team. Retrieved from the Bellevue University CIS 608 Classroom at http://www.bellevue.edu on September 14, 2011.

Baker, W. H., et al. (2010). 2009 Data Breach Investigations Report: A Study Conducted by the Verizon Business Risk Team. Retrieved from the Bellevue University CIS 608 Classroom at http://www.bellevue.edu on September 14, 2011.

Baker, W. H., et al. (2011). 2010 Data Breach Investigations Report: A Study Conducted by the Verizon Business Risk Team. Retrieved from the Bellevue University CIS 608 Classroom at http://www.bellevue.edu on September 14, 2011.

Bejtlich, R. (2006).Extrusion Detection: Security Monitoring for Internal Intrusions. Addison-Wesley: Upper Saddle River, NJ.

Dhanjani, N., et al. (2009). Hacking: The Next Generation. O'Reilly: Sebastapol, CA.

The Honeynet Project. (2004). Know Your Enemy: Learning About Security Threats, second edition. Addison-Wesley: Boston, MA.

Ligh, M. L., et al. (2011). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley Publishing, Inc.: Indianapolis, IN.

Parker, T., et al. (2004). Cyber Adversary Characterization: Auditing the Hacker Mind. Syngress: Boston, MA.

Ponemon Institute. (2009). Fourth Annual US Cost of Data Breach Study: Benchmark Study of Companies. Retrieved from the web at http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-

2009%20US%20Cost% 20of%20Data%20Breach%20Report%20Final.pdf on May 15, 2011.

Provos, N. and Holz, T. (2008). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley: Upper Saddle River, NJ.

Rash, M., et al. (2005). Intrusion Prevention and Active Response: Deploying Network and Host IPS. Syngress: Boston, MA.

Symantec. (2009) Anatomy of a Data Breach. Retrieved from the web at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf on September 17, 2011.

Trost, R. (2010). Practical Intrusion Analysis. Addison-Wesley: Upper Saddle River, NJ.

Wilhelm, T. and Andress, J. (2011). Ninja Hacking: Uncoventional Penetration Testing Tactics and Techniques. Syngress: Boston, MA.