2017

A review of data breaches and losses that occurred from laptops that were stolen or otherwise misplaced in 2015 and 2016

Samuel Griffith Wakeling
Edith Cowan University

Peter Hannay
Edith Cowan University

Zubair Baig
Edith Cowan University

DOI: 10.4225/75/5a84fc4395b51
Wakeling, S.G., Hannay, P., & Baig, Z. (2017). A review of data breaches and losses that occurred from laptops that were stolen or otherwise misplaced in 2015 and 2016. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.97-107).

A REVIEW OF DATA BREACHES AND LOSSES THAT OCCURRED FROM LAPTOPS THAT WERE STOLEN OR OTHERWISE MISPLACED IN 2015 AND 2016

Samuel Griffith Wakeling[2], Peter Hannay[1,2], Zubair Baig[1,2]
[1]Security Research Institute, [2]School of Science. Edith Cowan University, Perth, Western Australia
sgwakeli@our.ecu.edu.au, p.hannay@ecu.edu.au, z.baig@ecu.edu.au

Abstract

This paper provides an analysis of what information can be found on laptops that may or may not have connections to an organisation of some form, the statistics of the number of laptops stolen or otherwise misplaced in 2015 and 2016, and the number of potentially affected people from each of the cases. As seen in many news articles, laptops are often stolen or otherwise misplaced by employees or contractors in an organisational environment. As discovered in this research, many laptops are stolen from vehicles or homes of employees rather than organisation's buildings, but not all. The majority of stolen or otherwise misplaced laptops have very little information security on them, and this increases the risk of a data breach once a third party has physical access to the device. The research finds that, with available information, only one laptop had used encryption for the personal, private and confidential information that was stored on the internal storage device. In total, this paper finds that 33 laptops were stolen or otherwise misplaced in 2015 and 2016. The healthcare industry had the largest number of potentially affected people, with 5,352,792 people, and an average of 334,350 across the 16 laptops. The government sector had the second highest impact, with a total of 1,000,865 potentially affected people. Out of the 33 laptops, the total number of potentially affected people was 6,598,995 affected people, with an average of 83,702 potentially affected people with each of the 33 laptops.

Keywords: Laptop; Stolen; Misplaced; Data Breach; 2015; 2016

BACKGROUND

What information can be stored on laptops?

A computer device can contain a large amount of information, which with the correct software and hardware tools can be forensically analysed to find information of interest. This information can include:

- Temporary files:
  - Application data.
  - Web browser data.
- Active directory (AD) user account on organisational devices with an active directory server.
- Offline files from network drives, including drives configured with active directory.
- Network configurations:
  - Wireless credentials.
  - IP address configurations.
- User credentials
  - Organisational systems
  - Banking system
  - Social media
  - Session data
- Intellectual property
- Other personal information
  - Black mail potential

Temporary files can include data that is stored on a local system by an application. For example, a database application may store information that was retrieved or worked on from a database in the temporary files on the system. By analysing this data, it is possible that personal and private information may be available on the system in the temporarily stored files from the database system.

Web browser data can include session data for emails, databases or other systems that require authentication. This information, which is stored in cookies, could allow an attacker to bypass the authentication on a system by restoring a previously open session before the server times out the session. Research finds that some versions of Firefox are known to store cookies and other session data in a SQLite database (Pereira, 2009), which can easily be recovered with the correct tools.

An active directory (AD) system in an organisation copies a user's account files to the system that is used to log onto the domain (Microsoft, 2016). This account data can include any private and confidential documents that a user may have stored in their personal account. By analysing this data, an attacker could potentially gain access to confidential information from an organisation and gain access to temporary internet files for internal web pages in the organisation. The attacker could then view these pages to find any vulnerabilities in the services, and view the data from the active directory user account to see if there is any confidential information stored by the user in their account or their temporary files folders.

A computer device may be configured to store files offline from network drives or other shared folders (Microsoft, 2017a) in an organisation, either with or without an active directory server. This data can be analysed for confidential information that is stored on the organisation's internal servers that has been copied to the laptop's internal storage device.

A computer device may also contain network configurations for corporate networks, which attackers could use to determine how to continue gaining further access to the information systems at their target organisation. This network information can include wireless credentials that can allow attackers to connect other devices to the organisation's network and gain further access to information, as Windows allows users to view the wireless pre-shared key in plain text (Microsoft, 2017c) when they have physical access to the device.

Issues involved in the theft of laptops

All the information described above shows how much information could potentially be stored on a single device. If these devices are stolen or otherwise misplaced, a third-party individual or group could have access to a large amount of information. This could potentially allow them to leak more information than that found on the stolen device, as they could use configuration data to gain further access to the information systems on personal or organizational networks and gain access to more data.

With access to this device, the individual or group in possession of the device could leak any information they find on the device, and with the amount of information that could be stored on a single device, this has the potential to destroy the security reputation of an organization.

Furthermore, an attacker could install malicious code to a device, then attempt to anonymously return the device to the organization to attempt to back-door their way into the organization. If a re-obtained device is not thoroughly examined for additional code or applications running on the device, it could cause potential leaks of more confidential information from the organization.
Following the loss or integrity breach of this information and data, there are a number of potential outcomes, including:

- Data loss
    - Data being deleted and no longer being accessible or useable to the user.
- Data misuse
    - Data being used for purposes other than the intended use.
        - Fraud
        - Unlawful or unethical releases of private information
        - Black mail
- Data damage
    - Data being either corrupted or encrypted making it inaccessible while it still exists on the storage device.
- Reputation loss
    - Loss of data integrity reputation to the organisation or individual that was the subject of the data breach.
- Commercial advantage to a third party engaging in information warfare
    - The potential for another organisation to possess the research and other intellectual property created and stored by the user of the laptop.

RESEARCH METHOD

The statistics for this paper were gathered by using an advanced search in Google News specifying news articles only, dated from 01/01/2015 to 31/12/2015 with the keywords "laptop data breach". Google then returns news articles from laptops that were reported stolen or misplaced in 2015 with the potential information that may have been stored on them and how much data could have been breached. The search can also be limited to "Australia Only" to get news results for data breaches in Australia instead of worldwide. However, this does not yield enough results for this paper, and so this search limitation can be removed for further results.

These same search queries were run, but the dates were changed to starting at 01/01/2016 and ending at 31/12/2016 to obtain the statistics for laptops that were stolen or otherwise misplaced in 2016.

Only news articles that specify that a data breach occurred due to a laptop being stolen or otherwise misplaced are in the scope of this paper, other forms of data breaches, including network attacks, are not in the scope of this paper and will be ignored in the search results of news reports or articles.

To get the information to be compared, each article was examined, and the industry section, information about how many people are affected by the data breach, and if the device was secured and how will be entered into a table that will be used to compare the statistics from all newspaper articles found, with references.
From this gathered information, comparisons and discussions can be made about:

- The total number of data breaches from stolen or otherwise misplaced laptops in 2015.
- The total number of data breaches from stolen or otherwise misplaced laptops in 2016.
- The total number of people affected by the breaches in both 2015 and 2016.
- The average number of people per breach.
- The security in place on each of the stolen devices, and the security of the data on each of the devices.
- The average security setup for the laptops.

If any of the above information is unavailable, average calculations can be made for the total number of available statistics for each data type, or it will be assumed that zero people were affected by the unspecified breaches.

For the general information in this paper, other papers and technology webpages will be reviewed and cited for their information regarding the potential data that can be stored on laptops, based on their possible configurations and uses within or external to an organization.

DISCUSSION

What information can be retrieved from a stolen laptop and how?

When an attacker or another third party has physical access to a storage device from a laptop computer, they can easily gain access to the data that is stored on the disk. Utilizing many freely available forensic acquisition tools and utilizing the correct hardware, attackers or other unauthorized individuals or groups can view all of the data that is stored on the laptop in their possession, including data that has been deleted but the sectors have not yet been over-written. One method often used to retrieve this data is called file carving (Gladyshev & James, 2017).

Active Directory and other locally stored files

For example, if a laptop is connected to an Active Directory server, it will contain all of the information that the user has on any other system connected to that network. Assuming the device does not have encryption setup for the entire storage device, all of the information that has been downloaded from the Active Directory server will be visible in plain text. This can allow analyzers to easily scan for particular file types of interest or temporary database files. If an analyzer finds that files could have been deleted from the internal storage device on the laptop, with the correct hardware and software, the analyzer would be "able to recover the deleted files" (Hanson, 2005).
A laptop may also contain offline files from a network drive at an organization. The type of data that would be stored here would depend on the information that is stored on the network drive in the organization. However, this data can range from personal information to freely available data such as application installers.

A laptop may also have credentials stored on it, such as wireless network credentials or usernames and passwords for internal or external websites and systems in the organization. Even if these are not stored in plain text, they can be dictionary or brute-force attacked by a powerful system or rainbow table to find the original passwords. This task can be easily performed on another system once the storage device from the stolen or misplaced laptop is obtained, and there are a number of open source, free to use tools that can achieve this (Eston, 2010).

Web Browsers

Modern web browsers store a large amount of temporary data on a system. If a laptop is acquired, there may be open session data stored in the browser's temporary files and cookies, even if the user has attempted to delete them through their web browser (Pereira, 2009). This issue can allow an attacker to bypass the authentication systems on a web-based service and use the currently authenticated session on the device. With this session, an attacker could access more information stored on the network than just the information that was stored on the obtained device, and the attacker could potentially use this network access to launch more internal network attacks on the storage systems at the organization.

Many users also choose to allow their web browsers to save their login information to many web pages and services. This information can be harvested in order to obtain and dictionary or brute force attack the credentials utilizing tools such as John The Ripper (Taiabul Haque, Wright, & Scielzo, 2014), to re-use them to obtain more information from the network.

Web history data from web browsers can be used to determine what research was conducted on the laptop, or, what sites may have stored temporary information on the laptop. As temporary files are not often deleted, even if the user requests it (Pereira, 2009), there may be information of interest that can be obtained from recently viewed web pages that are in the browsing history of the device. Also, forensic tools can be used to view any temporary information that may have been deleted on the device.

User Directory

As discussed above, Active Directory servers will send a connected laptop a large amount of data or information from the storage systems from the network (Microsoft, 2016). However, if the system is not part of an Active Directory server, there may still be a large amount of information that is stored on the system while the user was working either on or off-site with data and information.

While the device is either at an organization or connected to the network with a Virtual Private Network (VPN), any documents or other information/data that are accessed on the remote storage servers may be temporarily stored on the local storage device in the laptop. This data can be harvested for any temporary data that might contain confidential information.

If an organization has a web-based document management system, such as Microsoft's SharePoint, there may be temporary downloaded documents stored in the user directory folder on the laptop's storage device. These files may contain completed forms or other records potentially containing confidential data or information.

Temporary internet files that are stored on the system from accessing the websites on the internal networks could be analyzed to find and potentially exploit any vulnerabilities that are present on the web server(s).

System Configurations

System configurations could be analyzed to determine the network structure of the organization and how it is configured. This data could be helpful for further network attacks that could be used to obtain more information than the information that is present on the laptop's internal storage device.

If the system is configured to access the internet through a proxy server, these credentials and connection information can be used to determine where the proxy server is on the network, and how to connect to it, which could be used by an attacker to redirect traffic to a different location. If an automatic configuration script is available on the system, it can contain this information (Microsoft, 2017d).

Wireless network credentials can also be stored on a laptop, and these can be retrieved from the laptop's internal storage device (Microsoft, 2017c). These credentials can be used to easily gain access to any wireless networks that the laptop has been connected to, including home networks and networks at organizations.

Laptops that have been connected to an organization may have network drives configured in the operating system (Microsoft, 2017b). The configuration information for these network drives can be used to determine the network and storage structure of the organization, as the network paths show up in the file browser. Also, some of these network drives may have been configured to store some information and data offline, and this information and data will be stored on the laptop's internal storage device.

STATISTICS OF STOLEN OR OTHERWISE MISPLACED LAPTOPS IN 2015

Table 1: of all cases in 2015

Industry	Number of potentially affected people	Was the device password protected?	Was the device encrypted?	
Background Screening	100,000	Password protected	Unencrypted	(Greenberg, 2015c)
Healthcare	39,090			(Snell, 2015a)
Education	9,300	Password protected	Not encrypted	(Leventhal, 2015)
Healthcare	8,000			(Muckenfuss, 2015)
Healthcare	3,000		Not encrypted	(Lewis, 2015)
Healthcare	2,800		Encrypted	(WISN, 2015)
Healthcare	1,359	Password protected	Not encrypted	(Cantu, 2015)
Education	941	Password protected	Not encrypted	(Gallagher, 2015)
Financial		Password protected	Not encrypted	(Ilascu, 2015)
Healthcare				(Snell, 2015b)
Healthcare			"All of the personal information contained on the laptop was deleted"	(Greenberg, 2015d)
Law				(Greenberg, 2015b)
Military			Encrypted	(Shropshire-Star, 2015)
Security			Encrypted	(Greenberg, 2015a)

Table 2: Data analysis of cases in 2015

Industry Sector	Total number of breaches	Average number of potentially affected people	Total number of potentially affected people
Background Screening	1	100,000	100,000
Healthcare	7	7,750	54,249
Education	2	5,121	10,241
Financial	1	0	0
Law	1	0	0
Military	1	0	0
Security	1	0	0
Total	14	16,124	164,490

As some of the articles or sources did not specify the number of potentially affected people, the calculations of total numbers in this table assumes that 0 people were affected on the cases with no data on the number of affected people for calculating the averages.

STATISTICS OF STOLEN OR OTHERWISE MISPLACED LAPTOPS IN 2016

Table 3: Total of all cases in 2016

Industry	Number of potentially affected people	Was the device password protected?	Was the device encrypted?	
Healthcare	5,000,000			(Barth, 2016)
Government	>1,000,000^			(Press Herald, 2016)

Military	130,000			(Bevan, 2016)
Healthcare	52,076	The device's networking and employee's credentials were disabled.		(Belliveau, 2016b)
Healthcare	<25,000#	Password protected		(Devlin, 2016)
Healthcare	12,000	Password protected		(Martin, 2016)
Education	4,022			(Monegain, 2016)
Healthcare	3,119			(Snell, 2016)
Sport	>1,000*			(Clarke, 2016)
Healthcare	600		"Patient information on the hard drive was encrypted"	(Belliveau, 2016a)
Aged care	75		The device was unencrypted	(Belfast Telegraph, 2016)
Education		Password protected.		(Whitbourn, 2016)
Healthcare		Password protected	Not encrypted	(Masters, 2016b)
Healthcare			Unencrypted	(Olenick, 2016b)
Prison		Password protected	Not encrypted	(Jayanthi, 2016)
Security		Password protected		(Olenick, 2016a)
Vacation Properties				(Masters, 2016a)

* Article only specified "thousands of players".
^ Article only specified "millions".
# Article only specified "up to 25,000".

Table 4: Data analysis of cases in 2016

Industry Sector	Total number of breaches	Average number of potentially affected people	Total number of potentially affected people
Healthcare	9	588,727	5,298,543
Government	2	500,432	1,000,865
Military	1	130,000	130,000
Education	2	2,011	4,022
Sport	1	1,000	1,000
Aged care	1	75	75
Prison	1		
Security	1		
Vacation Properties	1		
Total	19	135,805	6,434,505

As some of the articles or sources did not specify the number of potentially affected people, the calculations of total numbers in this table assumes that 0 people were affected on the cases with no data on the number of affected people for calculating the averages.

DATA ANALYSIS OF ALL STOLEN OR OTHERWISE MISPLACED LAPTOPS IN 2015 AND 2016

Table 5

Industry Sector	Total number of breaches	Average number of potentially affected people	Total number of potentially affected people
Healthcare	16	334,350	5,352,792
Government	2	500,432	1,000,865
Military	2	65,000	130,000
Background Screening	1	100,000	100,000

Education	4	3,566	14,263
Sport	1	1,000	1,000
Aged care	1	75	75
Security	2	0	0
Financial	1	0	0
Law	1	0	0
Prison	1	0	0
Vacation Properties	1	0	0
Total	33	83,702	6,598,995

As some of the articles or sources did not specify the number of potentially affected people, the calculations of total numbers in this table assumes that 0 people were affected on the cases with no data on the number of affected people for calculating the averages.

SUMMARY OF STATISTICS

An analysis of 33 different cases of laptops being stolen or otherwise misplaced found that a total of 16 of these were from the healthcare industry. The largest total number of potentially affected people with 5,000,000 potentially affected people in one data breach was from the healthcare industry. In these cases, the system was either protected with just a password or no security information was available. No encryption was used on the majority of the laptops in the cases.

Figure 1 shows the percentage of devices stolen from each sector. As shown in the diagram, 49% of cases occurred in the healthcare industry. The second largest industry was the education industry, with 12% of the cases.

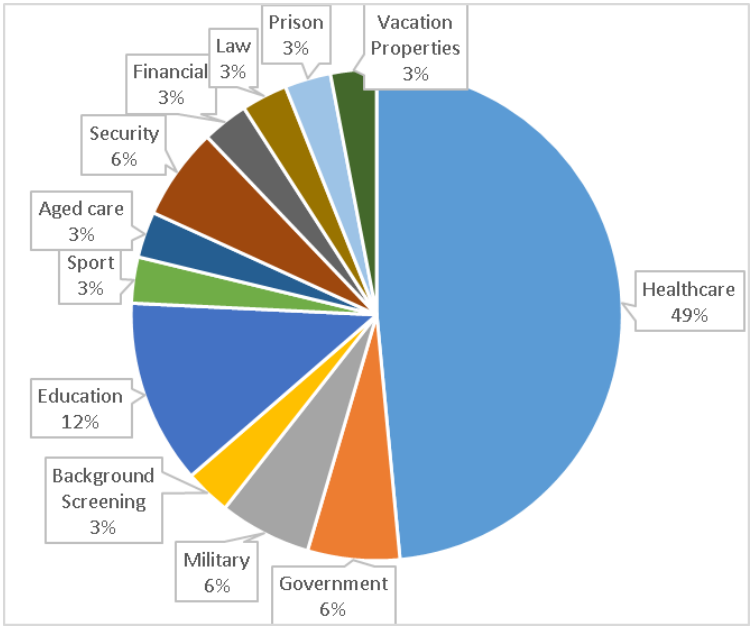

Figure 1: Number of cases

Figure 2 shows the percentage of people potentially affected in total by each industry sector. Healthcare had a total of 81% of the total number of potentially affected people, with the government sector following at 15% of the total number of potentially affected people.

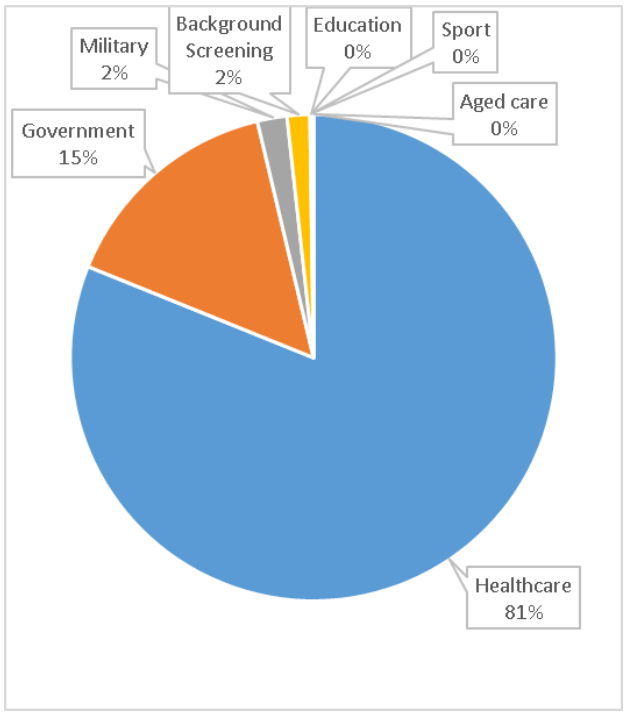

Figure 2: Number of potentially affected people

An analysis of available security information finds that there was no encryption used on the majority of laptops, and that they were simply protected with passwords in their operating systems. This means that all the information discussed in previous sections of this paper would be accessible in plain text, and an attacker can simply connect the storage device to another system or boot a live operating system on the stolen or misplaced laptop to gain access to the information on the system, allowing them to breach the integrity of the data of the potential number of affected people for each stolen or misplaced system.

CONCLUSION

In conclusion, this paper finds that very little security is used on laptops that contain personal information of employees or customers of businesses or other organisations. In some cases, the laptops belonged to the employees, rather than belonging to an organisation.

In total, the statistics of this paper finds that across the total of 33 analysed cases, an average of 83,702 people were potentially affected per stolen or otherwise misplaced laptop, with the total number of people potentially affected by stolen or otherwise misplaced laptops was 6,598,995 people.

The information in this paper can be used as a reference point for determining the security protocols that should be used on mobile devices, including but not limited to, laptops, phones, tablets and more. This paper's information is an example of the potential losses and breaches of integrity from a single stolen or otherwise misplaced unencrypted device from either an organisation or an employee's personal possessions.

Further research should be conducted yearly to monitor the statistics of stolen laptops, to check if data breaches from stolen or otherwise misplaced laptops continues to increase over time. If the statistics and information in this paper are used effectively in education and training, further research in this area should show a decline in the number of data breaches and potentially affected users from stolen or otherwise misplaced laptops in the future.

Further research over the past ten years should also be conducted to provide an accurate representation of the changes to the number of data breaches and people affected by stolen or otherwise misplaced laptops in the past, compared to the amount in 2015-2016 and the future. The data collected by all the research can be graphed and tabled for statistical and educational purposes with the intent to reduce the number of data breaches that occur from stolen or otherwise misplaced laptops in the future.

REFERENCES

Barth, Bradley. (2016). Personal laptop, possibly containing data on 5M patients, stolen from HHS facility. Retrieved 26-05, 2017, from https://www.scmagazine.com/personal-laptop-possibly-containing-data-on-5m-patients-stolen-from-hhs-facility/article/528761/

Belfast Telegraph. (2016). Nursing home fined for data breach after laptop with patients' details stolen. Retrieved 21-05, 2017, from http://www.belfasttelegraph.co.uk/news/northern-ireland/nursing-home-fined-for-data-breach-after-laptop-with-patients-details-stolen-34994692.html

Belliveau, Jacqueline. (2016a). Robbery at CA Practice Causes Possible Healthcare Data Breach. Retrieved 28-05, 2017, from http://healthitsecurity.com/news/robbery-at-ca-practice-causes-possible-healthcare-data-breach

Belliveau, Jacqueline. (2016b). Stolen Laptop Leads to Possible Healthcare Data Breach in KS. Retrieved 21-05, 2017, from http://healthitsecurity.com/news/stolen-laptop-leads-to-possible-healthcare-data-breach-in-ks

Bevan, Kate. (2016). 'Compromised' laptop implicated in US Navy breach of 130,000 records. Retrieved 21-05, 2017, from https://nakedsecurity.sophos.com/2016/11/24/compromised-laptop-implicated-in-us-navy-breach-of-130000-records/

Cantu, Tony. (2015). HealthSouth Rehab Hospital Warns of Potential Data Breach. Retrieved 19-09, 2017, from https://patch.com/texas/round-rock/healthsouth-rehab-hospital-warns-potential-data-breach-0

Clarke, Liz. (2016). Redskins employee's laptop stolen; NFL trying to determine extent of the breach. Retrieved 21-05, 2017, from https://www.washingtonpost.com/sports/redskins/redskins-employees-laptop-stolen-but-medical-records-not-feared-compromised/2016/06/01/3605b86e-2833-11e6-a3c4-0724e8e24f3f_story.html?utm_term=.25855e16c142

Devlin, Vince. (2016). Up to 25,000 could be affected by laptop stolen from New West employee. Retrieved 27-05, 2017, from http://missoulian.com/news/local/up-to-could-be-affected-by-laptop-stolen-from-new/article_88f2c565-a9dc-56f7-9620-25f4eb663d9b.html

Eston, Tom. (2010). Easy-To-Find Brute-Force Tools. InformationWeek(1284), 66.

Gallagher, Noel K. (2015). UMaine professor whose laptop was stolen violated university's data policy. Retrieved 25-08, 2017, from http://www.pressherald.com/2015/02/20/professor-whose-laptop-was-stolen-violated-university-systems-data-policy/

Gladyshev, Pavel, & James, Joshua I. (2017). Decision-theoretic file carving. Digital Investigation, 22(Supplement C), 46-61. doi: https://doi.org/10.1016/j.diin.2017.08.001

Greenberg, Adam. (2015a). Employee data on stolen Schlage Lock Company laptop. Retrieved 25-08, 2017, from https://www.scmagazine.com/employee-data-on-stolen-schlage-lock-company-laptop/article/532938/

Greenberg, Adam. (2015b). Personal data on laptop stolen from attorney with California law firm. Retrieved 25-08, 2015, from https://www.scmagazine.com/personal-data-on-laptop-stolen-from-attorney-with-california-law-firm/article/532899/

Greenberg, Adam. (2015c). SterlingBackcheck laptop stolen, contained data on about 100K individuals. Retrieved 25-08, 2017, from https://www.scmagazine.com/sterlingbackcheck-laptop-stolen-contained-data-on-about-100k-individuals/article/532911/

Greenberg, Adam. (2015d). Stolen DJO Global laptop contained patient data. Retrieved 25-08, 2017, from https://www.scmagazine.com/stolen-djo-global-laptop-contained-patient-data/article/536647/

Hanson, Doug. (2005). Computer forensic analysis. Law Enforcement Technology, 32(4), 8,10,12,14-16.

Ilascu, Ionut. (2015). Financial Institution Piedmont Advantage Loses Laptop with Customer Info. Retrieved 20-09, 2017, from http://news.softpedia.com/news/Financial-Institution-Piedmont-Advantage-Loses-Laptop-with-Customer-Info-474666.shtml

Jayanthi, Akanksha. (2016). Stolen laptop compromises PHI of California inmates. Retrieved 27-05, 2017, from http://www.beckershospitalreview.com/healthcare-information-technology/stolen-laptop-compromises-phi-of-california-inmates.html

Leventhal, Rajiv. (2015). University of Oklahoma Acknowledges Data Breach from Stolen Laptop. Retrieved 19-09, 2017, from https://www.healthcare-informatics.com/news-item/university-oklahoma-acknowledges-data-breach-stolen-laptop

Lewis, Dave. (2015). US Healthworks Suffers Data Breach Via Unencrypted Laptop. Retrieved 25-08, 2017, from https://www.forbes.com/sites/davelewis/2015/06/01/us-healthworks-suffers-data-breach-via-unencrypted-laptop/#2d9d57fb10c6

Martin, Kate. (2016). Stolen laptop tied to more than 12,000 accounts; CHI Franciscan says no evidence they were accessed. Retrieved 28-05, 2017, from http://www.thenewstribune.com/news/business/article122313219.html

Masters, Greg. (2016a). Laptop stolen from home of Welk Resorts employee, breach letters go out. Retrieved 27-05, 2017, from https://www.scmagazine.com/laptop-stolen-from-home-of-welk-resorts-employee-breach-letters-go-out/article/571096/

Masters, Greg. (2016b). Stolen laptop puts data of CVS customers in Alabama at risk. Retrieved 27-05, 2017, from https://www.scmagazine.com/stolen-laptop-puts-data-of-cvs-customers-in-alabama-at-risk/article/529115/

Microsoft. (2016). Folder Redirection, Offline Files, and Roaming User Profiles overview. Retrieved 20-09, 2017, from https://technet.microsoft.com/en-us/library/hh848267(v=ws.11).aspx

Microsoft. (2017a). Configure Offline Availability for a Shared Folder. Retrieved 10-10, 2017, from https://technet.microsoft.com/en-us/library/cc755136(v=ws.11).aspx

Microsoft. (2017b). Drive Map. Retrieved 11-10, 2017, from https://technet.microsoft.com/en-us/library/cc755136(v=ws.11).aspx

Microsoft. (2017c). How to find your wireless network password. Retrieved 29-09, 2017, from https://support.microsoft.com/en-us/help/4023501/surface-how-to-find-your-wireless-network-password

Microsoft. (2017d). Using Automatic Configuration, Automatic Proxy, and Automatic Detection. Retrieved 11-10, 2017, from https://technet.microsoft.com/en-au/library/cc985352.aspx

Monegain, Bernie. (2016). OHSU pays $2.7 million fine to HHS Office for Civil Rights for two HIPAA breaches. Retrieved 27-05, 2017, from http://www.healthcareitnews.com/news/ohsu-pays-27-million-fine-hhs-office-civil-rights-two-hipaa-breaches

Muckenfuss, Mark. (2015). UC RIVERSIDE: Computer stolen; data breach affects 8,000. Retrieved 25-08, 2015, from http://www.pe.com/2015/04/07/uc-riverside-computer-stolen-data-breach-affects-8000/

Olenick, Doug. (2016a). M. Holdings Security issues warning on possible data breach. Retrieved 27-05, 2017, from https://www.scmagazine.com/m-holdings-security-issues-warning-on-possible-data-breach/article/529460/

Olenick, Doug. (2016b). OptumRx customer records on stolen laptop compromised. Retrieved 28-05, 2017, from https://www.scmagazine.com/optumrx-customer-records-on-stolen-laptop-compromised/article/529045/

Pereira, Murilo Tito. (2009). Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records. Digital Investigation, 5(3), 93-103. doi: https://doi.org/10.1016/j.diin.2009.01.003

Press Herald. (2016). White House quiet about data breach. Retrieved 28-05, 2017, from http://www.pressherald.com/2016/04/04/white-house-quiet-about-data-breach/

Shropshire-Star. (2015). Laptop with MoD Donnington employee details stolen. Retrieved 20-09, 2017, from https://www.shropshirestar.com/news/2015/06/06/laptop-with-mod-donnington-employee-details-stolen/

Snell, Elizabeth. (2015a). ISMA Data Breach Reportedly from IT Head's Stolen Devices. Retrieved 20-09, 2017, from https://healthitsecurity.com/news/isma-data-breach-reportedly-from-it-heads-stolen-devices

Snell, Elizabeth. (2015b). PHI Safety Compromised After Texas Laptop Theft. Retrieved 19-09, 2017, from https://healthitsecurity.com/news/phi-safety-compromised-after-texas-laptop-theft

Snell, Elizabeth. (2016). Stolen Laptop Leads to Possible Health Data Breach in CO. Retrieved 26-05, 2017, from http://healthitsecurity.com/news/stolen-laptop-leads-to-possible-health-data-breach-in-co

Taiabul Haque, S. M., Wright, Matthew, & Scielzo, Shannon. (2014). Hierarchy of users′ web passwords: Perceptions, practices and susceptibilities. International Journal of Human-Computer Studies, 72(12), 860-874. doi: https://doi.org/10.1016/j.ijhcs.2014.07.007

Whitbourn, Michaela. (2016). Sydney University 'lost' computer containing sensitive student information. Retrieved 21-05, 2017, from http://www.smh.com.au/nsw/sydney-university-lost-computer-containing-sensitive-student-information-20160304-gnb4fa.html

WISN. (2015). Humana reports data breach that could affect up to 2,800. Retrieved 19-09, 2017, from http://www.wisn.com/article/humana-reports-data-breach-that-could-affect-up-to-2-800/6328907