Indian Journal of Information Sources and Services
ISSN: 2231-6094 Vol. 8 No. 2, 2018, pp. 8-11

Data Breach: Key to Prevention and Intrusion Detection the Risk of a Library

Indranil Sarkar
Librarian, Baluchar Primary Teachers' Training Institute, Murshidabad, West Bengal, India
E-Mail: ndrnlsarkar@gmail.com

Abstract **- The problem of protecting information and data flows has existed from the very first day of information exchange however advanced Information Communication Technology and information management systems become more and more powerful and distributed. In this article the author aver that the strategy need to implement measures to protect library from the rise of leak confidential information, both accidentally and maliciously, at tremendous cost in money, privacy, national security, and reputation.**
Keywords: **Security Breach, Dark Web, ITRC, VPN, PLA, Ransomware, Phishing**

I. INTRODUCTION

Modern Library have plethora of a computers with their physical Information Technology infrastructure like good bandwidth and servers with lots of space, mission statement (Intellectual freedom data privacy) and code ethics are very unique and strong. In the last few years, with a rise of web based ILS that can be accessed from anywhere and anytime with the help of World Wide Web. But there is a question about data breach. There are probably numerous technology solutions, both high tech and low, that can help to stop these situations from arising. Generally, library wanting to provide open access, they are target for a potential hackers, any past distinguished staff or non-log off computer left at an out event can be ripe for a data breach.[1]

Hundreds of thousands of area library users, including in Eau Claire, may have had their personal information stolen. On Friday, Sept. 15, 2017 Indianhead Federated Library System, a consortium of public libraries that covers 10 countries including Eau Claire and Chippewa, learned a data breach had occurred. According to Indianhead representative, they have 240,000 library patron records on file. In a release, Information from more member library patron records that were obtained by an "Unauthorized Party" included Library patron barcodes, Telephone numbers, Names, Addresses, Email addresses, Birth dates, Identification record numbers, such as driver's license number.

Indianhead Federated Library System stated those who may have been affected by the breach were notified by mail. [2]

II. OBJECTIVE OF THE STUDY

1. To find out the biggest data breaches in 21st Century
2. To find out a records of stolen data in the year of 2017
3. Learn about three major strategies need to be protecting of library data breach
4. Learn about what other threats abound
5. To study the 2017 semantic threat report for online threats.

III. BIGGEST DATA BREACHES OF THE 21ST CENTURY

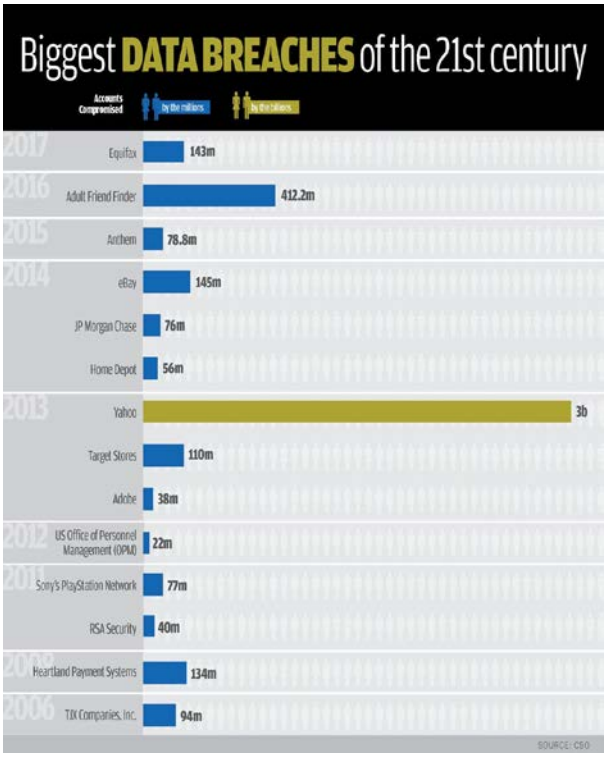

Fig. 1 Biggest Data Breaches

List of handy information about major data breach carried out by Wikipedia. With a minimum searching last few years there has been data breach given below. With a vast majority of data breaches originating from inside the organization rather than malicious attacks by out siders-it's vital to be monitoring outside the firewall for any signs of data being leaked, breached or sold. Although some of this data inevitably cant traced, a common mechanism for data breaches is data to be leaked, marketed or sold on the dark web or invisible web. [3]

IV. RECORDS BREACHED IN THE YEAR 2017

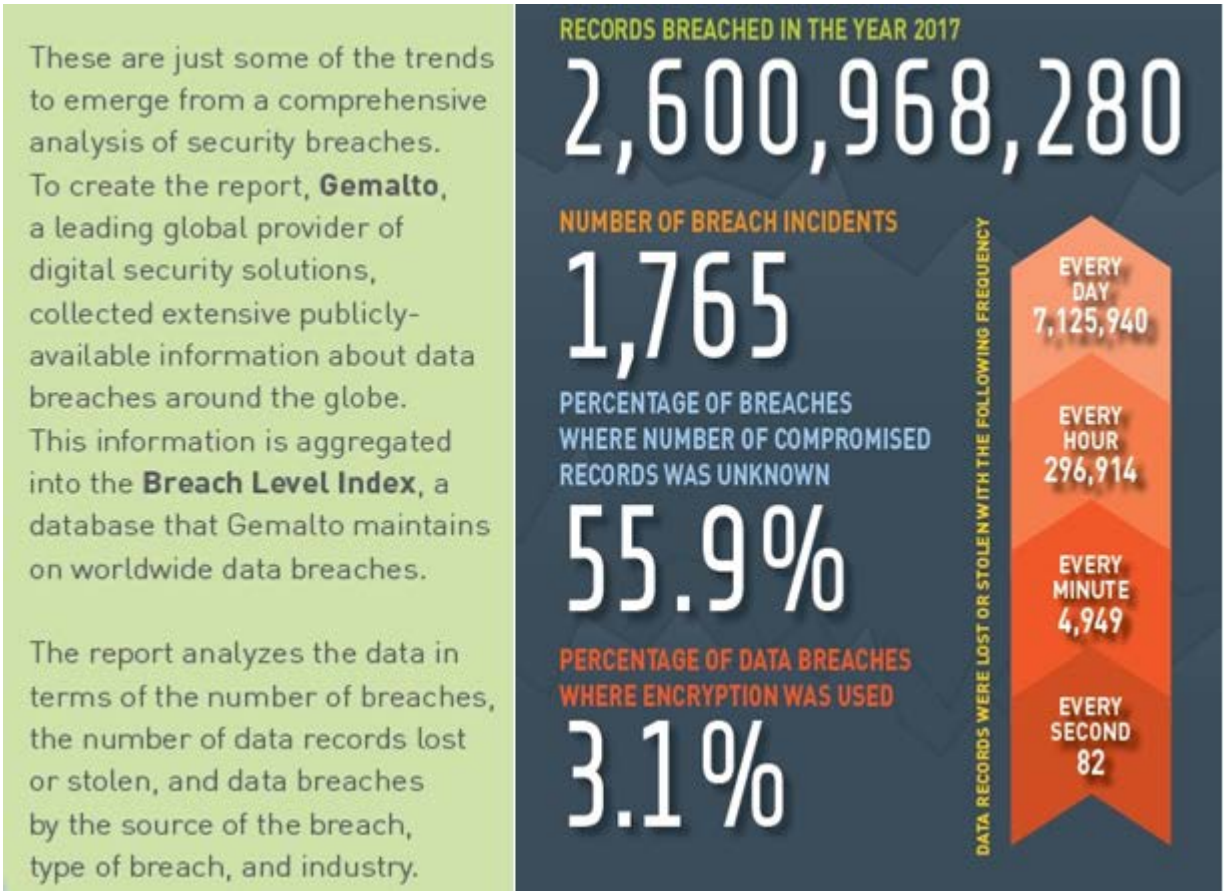

Fig. 2 Breaches in the year 2017

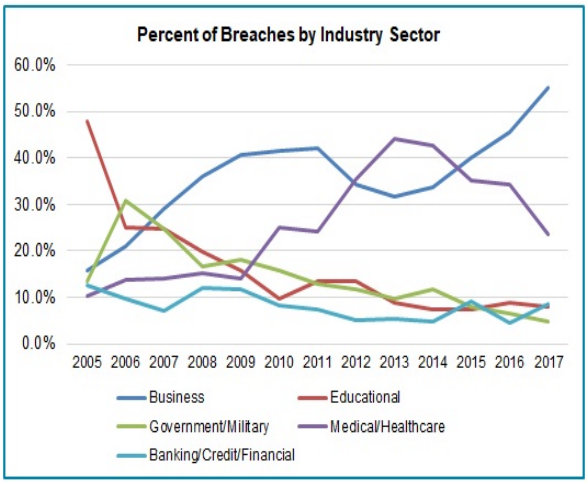

Fig. 3 Percent of Breaches by Industry Sector

Of the five industry sectors that the Identity Theft Resource Center (ITRC) tracks, the business category again topped the ITRC's Data Breach List for the third year in a row with 55 percent of the overall total number of breaches (870). This marks the eighth time since 2005 that the number of breaches for this sector has surpassed all other industries. The Medical/Healthcare industry followed in second place with 23.7 percent of the overall total number of breaches (374). The Banking/Credit/Financial sector rounds out the top three with 8.5 percent of the overall total (134). This is only the second time since 2005 that the Banking/Credit/Financial sector has ranked in the top three industry categories. The remaining two sectors, Educational and Government/Military, represented 8 percent and 4.7 percent respectively. [5]

V. THREE MAJOR STRATEGIES NEED TO BE PROTECTING OF LIBRARY DATA BREACH

A. Prevention Strategy

Library can prevent many threats by implementing an overall security policy and frequent communication to ensure users are educated. Prevention best practices include:

1. Strong Password: Firstly start with the basic – password. Keep your password secret (Never ever write them down), use different password with mix of numbers, letters, special character's and change them regularly.
2. Two-Step Verification: As always double check the authenticity of any one reaching out to you regarding what could be deemed sensitive information, by it via email, phone or otherwise.

3. Educate Patron and Staff on Cyber Security Risk: Educate patron and staff on the overall need for the security. Highlight how small, unassuming actions like opening strange email can lead to drastic consequences. Requiring Virtual Private Network (VPN) to security accesses library system for more technical system managers, librarians. VPN encrypt data while in transit and offer other layer of protection that can be unlocked with a code kept in an online vault.
4. Cyber Security Awareness: As the need for cyber security awareness grows, public libraries are stepping up efforts to provide critical digital literacy training and information. Public Library Association is doing its part by highlighting cyber security material on DigitalLearn.org a collection of self-directed, interactive online tutorials developed by the association to help users increase their digital literacy. At DigitalLearn.org, learners can take short, self-directed courses that help them recognize danger and stay safe online. These include:
    a. *Accounts and Passwords:* This course teaches how to create safe online accounts, including creating secure passwords and keeping accounts secure.
    b. *Online Scams:* This course helps new computer users identify and recognize types of scams, how to avoid getting hurt, and how to report them.
    c. *Internet Privacy:* This course helps learners understand the level of personal, confidential information we can share on websites and via email, and take control of the information we are constantly sending and receiving.

5. Secure Protocol: Access internal sites via Hyper Text Transfer Protocol Secure protocol for extra safety.
6. Perimeter Security on Firewalls: Apply perimeter security on firewalls for 'state-full' scan of content frequency, volume and sequences, as well as destination domains address known to be troublesome, enables intelligent judgment to protect systems.

Use the complementary white/blacklist capability provided through reputable email vendors delivers or quarantines email accordingly. [6]

B. Detection Strategy

To help organisations identify breaches sooner, breach detection platform provider Last line lists seven tips:

1. *Bring in Cyber Security Experts:* It sounds obvious, but employing people who know what they're doing is essential for effective cyber security. However, finding them can be hard, and it will only get harder, according to $(ISC)^2$. The organisation released a report in February 2017 claiming that the cyber security skills gap will grow to 1.8 million by 2022.
2. *Stay Up to Date:* The cyber threat landscape is constantly evolving, so it's important that your organisation evolves with it. This means making sure your employees and technology are up to date with new attack methods and the ways criminals exploit organisations.
3. *Use Data Breach Detection Tools:* As well as maintaining systems, servers and applications, organisations need to have in place modern breach detection tools. Lastline writes: "Although security budgets have increased during the last few years, many organisations are still purchasing and deploying old technology. Unfortunately, these legacy products are no longer effective at preventing modern breaches."
4. *Use Global Threat Intelligence:* According to The SANS State of Cyber Threat Intelligence Survey, organisations that use global cyber threat intelligence have faster and more accurate response times and are better equipped to identify, detect and prevent new threats.
5. *Organisation Monitoring:* To detect and investigate security incidents more effectively, security analysts need to be able to see the key indicators of compromise. This includes network-level telemetry, logs and events from underlying infrastructure, applications and security systems.
6. *Monitor Attack Campaigns:* Conventional malware detection products only allow you to see point-in-time threats, generating notifications as individual events occur. This often means security analysts are left chasing an endless number of irrelevant alerts. Organisations that focus on attack campaigns, not just individual alerts, are able to spot breaches early.
7. *Provide Regular Staff Awareness Training:* Negligence is often a huge factor when it comes to breaches. Organisations should provide all their employees with regular training on how to identify attacks and vulnerabilities, and what they should do next. Training should occur at least annually, or following any security incident.

C. Recovery Strategy

All library systems- servers, applications, storage and even integrated library system (ILS) - are suspect able to hacking. If a breach occurs, taking action to minimize impact and ensure a quick and safe recovery is essential. Automate the data backup function to maintain a recent copy of data. Set backups to occur at certain times of the day, or when triggered by milestone's or specific events. For examples reaching a threshold of newly issued library cards or hosting a number of jobs training events where patrons input data could activate a backup. Perform routine testing of backup to ensure they are successful. Follow the 3-2-1 backup strategy in which there are always three copies of critical data: two on different media or devices and offsite.

VI. THREATS ABOUND

Ransomware is one of many types of attacks that can occur via desktop computers, laptops, tablets, mobile phones, apps, websites and email. The resulting loss of data, identities, privacy and even systems creates significant

disruption. Other common, malicious software programs include:

1. Viruses: These reproduce and spread to corrupt systems and destroy data.
2. Worms: This form of malware takes advantage of security failures to consume bandwidth and harm networks.
3. Trojan Horses: These are triggered by clicking on ads, downloading files, or accessing harmful links in email or text messages.
4. Denial of service: This occurs when a website is overloaded with traffic, preventing or grinding functions to a halt.
5. Phishing: This attack happen when transactions appear to process normally, but in the background data is captured, viruses are deployed and hackers gain future access. [7]

VII. ONLINE THREATS

1. 4000 ransomware attacks every day.
2. 78% of people aware of risk from unknown
3. 21% of organizations trace data breaches to bring your own device programs.
4. 140 days is the average time attackers hide in a network.
5. 44% of network connected printers are insecure. [8]

VIII. CONCLUSION

Today data is considered as valuable as gold. No one is 100% safe from cyber hackers in a digital world. ITRC reported in 2017 that the top of data breach occurred in the business category. In this paper presented that the best way key techniques to preventing and detecting data breach in the library require constant effort and also pointed out numerous data breach happens in the world.

REFERENCES

[1] Lyttle, M. A., Walsh, S.D. (2015, March 20). Protecting your library against data breach. Retrieved May 23, 2018, from http://publiclibrariesonline.org/2015/03/protecting-your-library-against-a-data-breach/

[2] Library patrons in 10 western Wisconsin countries affected in data breach. Retrieved May 26, 2018, from http://www.week.com/story/36583282/2017/10/Thursday/alert-library-patrons-in-10-western-wisconsin-counties-affected-in-data-breach

[3] Armerding, T. (2018, January 26). The 17 biggest data breaches of the 21st century. Security practitioners weigh in on the 17 worst data breaches in recent memory. Retrieved May 24, 2018, from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[4] Gemalto. (2017). The year of internal threats and accidental data breaches. Retrieved May 27, 2018, from https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

[5] Cyber scout. (2017). ITRC: 2017 Annual data breach year-end review Retrieved June 6, 2018, from https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

[6] Maxfield, D. (2017, October 19). Technology & Data Security in Libraries: A Playbook for Managing today's Imperative. Retrieved May 28, 2018, from http://www.governing.com/topics/education/technology--data-security-in-libraries-a-playbook-for-managing-todays-imperative.html

[7] Irwin, L. (2017, December 12). 7 tips for spotting a data breach. Retrieved June 2, 2018, from https://www.itgovernance.eu/blog/en/7-tips-for-spotting-a-data-breach

[8] Semantec. (2017). Internet security threat report. Mountain view, CA: Semantec Corporation, USA. Retrieved May 28, 2018, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf