Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.4, No.3, 2013

System and Data Capture Framework Insights into Breach Data toward Improved Feedback

Adewale O Adebayo* Yinka A Adekunle Olawale J Omotosho
School of Computing and Engineering Sciences, Babcock University, P.M.B.21244 Ikeja, Lagos, Nigeria
* E-mail of the corresponding author: adebayoa@babcock.edu.ng; wale_adebayo@yahoo.com

Abstract

A secure information infrastructure is required to sustain competitive advantage. Despite creditable efforts, there are visible failures of Information Security (IS). Breach data offers necessary relatively unbiased and robust feedback to reveal what is overlooked for apt countermeasures and improved IS decisions. None of the previous works done analyzing breach data critically examine the process of breach data capture and reporting system, and breach data capture frameworks from a holistic perspective for improved substantive feedback, which this work addressed. A model of breach data capture and reporting system was proposed through argumentation and a fluid iterative cycle of awareness, suggestion, development, evaluation and conclusion. A breach data capture framework was proposed through argumentation and examination of existing related frameworks, employing the fluid iterative cycle, while fostering acceptability. The framework was evaluated in comparison with existing breach data capture frameworks. The proposed model and framework are complimentary efforts for substantive feedback toward apt countermeasures and improved IS decisions.

Keywords: Model, data capture framework, breach data system, breach data capture, framework.

1. Introduction

Information is essential to the continued growth of any society. A secure information infrastructure is required to sustain competitive advantage. Despite credible efforts taking holistic approaches (Peltier, et al., 2005; Martin & Weadock, 1997), some generally visible failures of information security (IS) are spam and associated problems (Helbush, 2009), malicious codes (Eichin & Rochlis, 1989), bugs in software including operating systems (Keizer, 2010), and data breaches (Aitoro, 2007). Notable failings of IS (FBI, 2010; Helbush, 2009; SonicWALL, 2008; Klienman, 2007; FBI, 2007; Gartner, 2007), IS industry not currently organized for IS leadership (Gordon, Loeb and Sohail, 2010; Johnson, et al., 2010; Baskerville & Myers, 2009), and inadequacies of existing evidence to support IS decision making (Shostack & Stewart, 2009; Hoffer & Straub, 1989) are cogent reasons for fresh perspective to the subject of IS. The use of breach data and other new sources of data that would eliminate or reduce some of the setbacks of survey in IS (Ryan and Jefferson, 2003), and would provide new perspective to the subject of IS were proposed (Mahmood, et al., 2010; Shostack and Stewart, 2009). The breach data by its nature offers widely spread, unbiased, and easily accessible data for analysis to provide fresh insight into issues surrounding data breaches and therefore IS. Breach data is gathered and shared at PogoWasRight.org, Attrition.org, Privacy Rights Clearing House, and other sites (Shostack & Stewart, 2009, p187; Adebayo, 2012). Information security system feedback is essential in improving the system through further controls. Control entails observation, assessment, intervention, and communication line between observation, assessment, and intervention (Anthony, Dearden, and Bedford, 1984). The breach data offers the essential feedback that IS professionals would use to assess how well their security measures are doing, and what necessary apt intervention to apply.

A number of works have been done analyzing breach data (Adebayo, Omotosho and Adekunle, 2012; Gordon, et al., 2010; Culnan & Williams, 2009; Hasan & Yurcik, 2006; Acquisti, Friedman and Telang, 2006; Tehan, 2005) and its repositories (Adebayo, 2012), but none yet examined breach data capture frameworks, and no model exists to shed light on and provide basis for improving the information security feedback system of breach data. There is the need to examine breach data capture frameworks toward a common language for describing data breach incidents in a structured and repeatable manner. This will ensure proper and consistent data capture that would be consolidated or accumulated to yield much more feedback benefits, and would ensure that what is ultimately analyzed contains

essential details in the right format necessary for enlightenment about IS situation for improved pathway forward and apt intervention to forestall data breaches. There is also the need to make vivid the process of breach data capture and reporting system to improve the feedback system. The goal of this work was, therefore, to provide system and data capture framework insights into breach data toward improved countermeasures against storage security breaches. The coincidental applicable research questions were: What model is appropriate for breach data capture and reporting system? What is appropriate framework for breach data capture and reporting system toward improved IS decisions?
The model should serve as a basic guide to breach data capture and subsequent usage system design. The framework should provide basis for continued proper capturing of breach data thereby providing more useful feedback.

1.1 Methods of the Research

The design and creation of the model went through argumentation and a fluid iterative cycle of awareness (recognition and articulation of a problem), suggestion (leap from curiosity to offering a very tentative idea for solving the problem), development (tentative idea is developed), evaluation (assessment of the developed for its worth and deviations from expectations), and conclusion (Vaishnavi & Kvechler, 2004). An extensive literature review was performed. Search terms, including model and system, were used on search engines, and available hard documents on these matters were sought. The relevant documents obtained were qualitatively analyzed for convergence, essentials, determinants and expositions, using inductive approach. The model main factors and events, and their relationships were logically identified, and proposed through argumentation. The model was subsequently objectively and graphically checked to be sure it captures the necessary and essential ingredients for its purposes. It was also examined to depict and simplify reality, and make it more understandable. Finally, the model was evaluated in terms of functionality and completeness.
Design and creation of a prototype breach data capture framework went through a fluid iterative cycle of awareness, suggestion, development, evaluation, and conclusion. An extensive literature review was performed. Search terms, including framework and threat model, were used on search engines, and available hard documents on these matters were sought. The relevant documents obtained were qualitatively analyzed for convergence, essentials, determinants and expositions, using inductive approach. The main actors and their sub-classes of the framework were logically identified (Breach incident data capture framework should translate the incident narrative of "who did what to what (or whom) with what result" into a form more suitable for trending and analysis ([Online] Available: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, 15/4/12)). The prototype framework was subsequently objectively and graphically checked to be sure it captures the necessary and essential ingredients for its purpose. The prototype framework provides bases for the development of a frame for breach data capture. The found breach data capture frameworks were examined in terms of fit for purpose, sufficiency, adequacy, completeness, simplicity and acceptability, and were consolidated, focused, innovated and complemented by ingenuity to achieve the proposed, while fostering acceptability in the light of what is required to be made public by the law regarding the breach of personally identifying information. The outcome was then evaluated in comparison with existing breach data capture frameworks.
No exceptional difficulty of being an ethical researcher was encountered.

2. Outcomes

In this section are proposed a model to shed light on and provide basis for improving the information security feedback system of breach data, and a breach data capture framework.

2.1. The Proposed Model

A model is a valid representative of something for the purposes desired. It captures the determining factors, together with their relationships, of the system of interest.
Information security measures are applied to and/or built into information infrastructure to make it function as intended in the face of smart adversaries. Whenever there is a security breach, it is an indication that the measures

need improvement. Informative feedback on the breach incident helps inform apt security measures, thereby leading towards a safer computing environment and experience (Figure 1).
With the wisdom of hindsight of breach data repositories study and related works, a model of security breach incident data capture and reporting system is presented (Figure 2).
Breach incidents details are captured based on particular framework. Security breaches known countermeasures are captured based on categories of threats determined by breach countermeasure capture framework that is based on breach incident data capture framework.
Data is analyzed to inform about what appropriate countermeasure, apt measure, mitigation effort, remedial effort or other, to accentuate in preventing future occurrences and stemming the current incident. This then informed the inclusion of prescribed countermeasures for each kind of particular event within incident. Countermeasures are known things suitable for counteracting attack events. Response time would be shortened if these countermeasures are relayed together with incident reports. These details are processed to generate pointed reports showing what had happened and what should be done.
Organisations sharing the same data capture framework could merge data and be better informed. A worldwide acceptance of a framework would yield far reaching information towards a safer computing environment when organisations merge data.
There is the need also to limit, stem and stop a currently noticed breach. The forensic investigation system, which is included, serves this purpose. The life cycle of a forensic investigation includes initial evidence, creation of indicators of compromise (IOC) for host and network, deployment of IOCs in the enterprise, identification of additional suspect systems, collection of evidence, analysis of evidence, refinement and creation of new IOCs, and remediation. Madiant IOC Editor and Madiant IOC Finder are joint open tools, while Madiant Intelligent Response is a commercial tool, for forensic investigation (openioc.org/resources/An_Introduction_to_openIOC.pdf & www.openioc.org, 2/9/12).

2.2. The Proposed Breach Data Capture Framework

The study of breach data repositories and related works revealed that there are four basic entities regarding any breach incident. They are the incident agent, the method used by the agent, the asset of target, and what was done or could have been done to the asset. The relationships of these basic entities, including the incident, are depicted in Figure 3.
In addition to these basic entities are their categories or types, as well as their sub-types and subsequent sub-types and so on. Figure 4 shows subsequent relationships for any basic entity.
Specificity should be imposed. The reason for specificity, limiting entries to selecting from certain options, is to enable consistent meaningful data capture. This will make visualizing a layered approach to deterring, preventing, and detecting the incident possible. Allowing much free text entries would obscure and introduce difficulty in processing for useful reports.
Each possible attribute of a breach entity should consist of detail levels class, family, component and element. Class is a general grouping having general focus. Family is a more specific focus but differ in emphasis and rigour. Component is smallest selectable unit. Element is lowest level of expression of a security breach that is verifiable by investigation (Common Criteria for Information Technology Security Evaluation, www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf, 9/2/13). It is not compulsory that every class most necessarily have family, every family a component, nor every component an element, and the need for a sub-class beyond element is an indication of an absent class to be created.
This prototype framework is a fit and functional frame, to ensure the proper capture of all relevant details of a breach incident for analysis toward improved feedback.

The proposed essential attributes (class, family, component and element) of a data breach incident (breach incident), the person who caused the incident to happen (breach agent), the method(s) used or what was done by the agent (breach method), the asset abused (breached asset), and what happened about or to the asset (Content breached), in the light of what are made public and engendering acceptability, are provided below.

2.2.1. Breach Incident Attributes

The breach incident classes are be Victim and Tracking. Victim class family consists of Organisation's name, Organisation's Head-office address (country and town components), Organisation's web address, Organisation's Industry or primary sector (North American Industry Classification System components - www.census.gov/eos/www/naics/ components), and Organisation's location (country and town components), and any other organisation related information.

Tracking class family should be Incident unique identifier, Source(s) of incident information, Discovery method (External (Customer, Audit, and Other elements), Internal (user, audit, surveillance, and other elements) and Unknown components), Dates (incident occurred, incident discovery, organisation reported incident, and organisation mail notification components), Incident summary, and Notes/Attachments.

2.2.2. Breach Agent Attributes

The breach agent classes are Outsider/External (unknown, stakeholder, market forces, criminal group, nation/state sponsored, and other families), Insider/Internal (information system expert, management, auditor, and other families), Third-party/Partner/Contractor (type (information system expert, and other components), and origin families), Unknown, Undisclosed, Motive (accidental/unintentional, intentional, unknown, no further information, and other families), and any other agent related information class.

2.2.3. Breach method Attributes

The breach method classes are Hacking, Social (phishing, forgery, scam, pre-texting, unknown, and other families), Physical (theft (data recovered component (yes and no elements), sabotage, skimming, assault, unknown, and other families), Misuse, Error (loss, delivery, accident, web exposure, disposal, unknown, and other families), Environmental, Unknown, and Other.

2.2.4. Breached asset attributes

The breached asset classes are Type (Employee (information system expert, management, auditor, and other components), Media (hard copy, hard drive, disk, and other components), server (database, and other components), Personal computer (laptop, desktop, tablet, and other components), Unknown, and Other families), and Location (internal, external, and other families). This is shown graphically in Figure 5.

2.2.5. Breached Content Attributes.

The Breached Content classes are Confidentiality (Data Type (name, address, credit card number, social security number or equivalent, email address, medical, date of birth, financial, accounting, miscellaneous, unknown, password, phone number, username, intellectual property, and other components), Number of Records lost, and Data state (unencrypted, encrypted, and unknown components) families), and Possession/availability (loss and other families).

3. RELATED WORKS

A US federal data breach notification and reporting law could fulfil the need for a common vocabulary for describing security breach related issues with attendant benefits, though many argue that it is untenable ([Online] Available: http://www.myid.com/blog/the-debate-over-data-notification-laws-returns/, 23/4/12).
The following are notable existing breach data capture frameworks presented in consistent structure.

3.1. Open Security Foundation Breach Data Capture Framework.

Breach Incident Attributes - The breach incident classes are Victim and Tracking. Victim class family consists of Organisation's name (primary and third-party components), Organisation's Head-office address (primary (country and town elements), and third-party (country and town elements) components), Organisation's web address, Organisation's location, Organisation's primary sector (Business, Education, Government and Medical components), and any other organisation related information. Tracking class family are Incident summary, Arrest (Yes or No components), Law Suit (Yes or No components), Data Recovered (Yes or No components), Dates (incident occurred, incident discovery, organisation reported incident, and organisation mail notification components), Source(s) of incident information, Attachments, and Notes/Additional information.
Breach Agent Attributes - The breach agent classes are Outsider, Insider Accidental, Insider Malicious, Insider- no further information, and Unknown.
Breach Method Attributes - The breach method are Virus, Hacking, Social (fraud and snooping families), Error (loss, email, disposal, and web exposure families), Physical (theft, postal, fax, disposal, and skimming families), and Unknown.
Breached Asset Attributes - The breached asset classes are Electronic (laptop, computer, media (tape, disk and drive components), and mobile families), Document, Other and Unknown.
Breached Content Attributes - The Breached Content class is confidentiality/Possession (data type (name, address, credit card number, social security number or equivalent, email address, medical, date of birth, financial, accounting, miscellaneous, unknown, password, phone number, username, intellectual property, and other components), and Number of Records lost family) (www.DataLossDb.org./submissions/new, 9/2/13).

3.2. Identity Theft Resource Centre Breach Data Capture/Reporting Framework.

Breach Incident Attributes - The breach incident classes are Victim and Tracking. Victim class family consists of Primary Industry (business, financial/credit/banking, educational, government/military, and health care/medical components), Company/Agency name, and Victim's state in US. Incident tracking class family consists of Breach identifier, Source, Discovery date, Record Involved (Yes or No components), and Incident summary.
Breach Agent Attributes - The breach agent classes are Insider, Outsider, and Subcontractor.

Breach Method Attributes - The breach method classes are Hacking, Accidental exposure, and Theft.
Breached Asset Attributes - No Breached Asset class exits.
Breached Content Attributes - The Breached Content class is Confidentiality (Data on the move, and Number of Records exposed family) (www.idtheftcenter.org/ITRC Breach Stats Report 2012.pdf, 9/2/2013).

3.3. Infosecurityanalysis.com Framework.

Breach Incident Attributes - The breach incident classes are Victim and Tracking. Victim class family consists of Organisation's name, Organisation's location (country and town components), Organisation's Industry/Vertical (Business (Technical, Financial and Retail elements), Education, Government and Health components), and Public/Private (public and private components).

Tracking class family are Date of incident discovery, and Description of incident.
Breach Agent Attributes - The breach agent classes are Malicious Insider/Employees, Third-party, Careless/Untrained employees/Insiders, and Hacker.

Breach Method Attributes - The breach method classes are Worm/virus, Hacking, Theft, Error (Loss, accidental, and exposure families), and Unknown/not disclosed.
Breached Asset Attributes - The breached asset classes are Media (electronic, paper, and not specified components), Laptop, and location (not specified, external, and internal components).
Breached Content Attributes - The Breached Content class is Number of Records.

3.4. Privacy Rights Clearing House Framework.

Breach Incident Attributes - The breach incident classes are Victim and Tracking. Victim class family consists of Organisation type (Business (Other, Financial and Insurance, and Retail/Merchant elements), Education, Government/Military, Healthcare, and Non profit components). Tracking class family has no value.
Breach Agent Attributes - The breach agent is simply Insider-intentional.
Breach Method Attributes - The breach method classes are Error (Loss, Disclosure, and Disposal components), Hacking/Malware, Theft, Payment Card fraud, and Unknown.
Breached Asset Attributes - The breached asset classes are Media (Compact disk, Hard disk, flash, memory card, tape, and non-electronic families), Potable device (laptop, personal digital assistant, smart phone and other families), and Stationary device (personal computer, and server families).
Breached Content Attributes - The Breached Content attribute was unaddressed (https://www.privacyrights.org/data-breach, 21/1/13).

3.5. Office of Inadequate Security Framework.

Breach Incident Attributes - The breach incident classes are Victim and Tracking. Victim class family consists of Organisation Class (Business, Education, Financial, Government, Healthcare, and Miscellaneous components), and Organisation region (US, and Non-US components). Tracking class family has no value.
Breach Agent Attributes - The breach agent classes are insider, Outsider, and Sub-contractor.
Breach Method Attributes - The breach method classes are Error (Exposure, and Loss/missing components), Hacking, Malware, Physical (Theft, and Skimming components), Misuse-Unauthorized access, and Other.
Breached Asset Attributes - The breached asset attributes are uncategorized except paper.
Breached Content Attributes - The Breached Content attribute was unaddressed (www.Databreaches.net, 9/2/13).

3.6. Verizon Enterprise Risk and Incident Sharing (VERIS) Framework.

Breach Incident Attributes - The breach incident classes are Victim Demographics and Incident Tracking. Victim demographics class family consists of victim identifier, primary industry (North American Industry Classification System components; www.census.gov/eos/www/naics/), victim location, number of employees (1 to 10, 11 to 100, 101 to 1000, 1001 to 10000, 10001 to 25000, 25001 to 50000, 50001 to 100000, Over 100000, and Unknown components), annual revenue, and notes. Incident tracking class family consists of Incident identifier, Source, whether confirmed (Confirmed, Suspected, and No components), Discovery method (External (threat agent, fraud detection, managed security event monitoring service, law enforcement, customer/partner, and unrelated party elements), and Internal (security audit/scan, antivirus alert, separate incident response, financial audit, fraud detection mechanism, host IDS or file integrity monitoring, IT audit or scan, log review process or SIEM, network IDS or IPS alert, physical security system alarm, reported by user, Unknown, and Other elements) components), Investigation start date, Incident summary, related incidents, and confidence rating (High, Medium, Low, and None components).
Breach Agent Attributes - The breach agent classes are External (Activist, Auditor, Competitor, Customer, Force majeure, Former employee, Nation-state, Organized crime, Acquaintance, State-sponsored, Terrorist, Unaffiliated, Unknown, and Other families), Internal (Auditor, Call centre, Cashier, End-user, Executive, Finance, Helpdesk, Human resources, Maintenance, Manager, Guard, Software developer, System or network administrator, Unknown, and Other families), Partner (type (North American Industry Classification System components), and origin (country list components) families), Role (Unintentional action, Espionage or competitive advantage, Fear or duress, Financial or personal gain, Fun, curiosity, or pride, Grudge or personal offense, Ideology or protest, Unknown, and Other families), Motive (Malicious, Inappropriate, Indirect, Unintentional, Conditional-Unintentional, and Unknown families), and Note.
Breach method Attributes - The breach method classes are Malware (Variety (Adware, Backdoor, Brute force, Capture data from application or system process, Capture stored data, Client-side or browser attack, Command and control, Destroy or corrupt stored data, Disable controls, Denial of Service, Downloader, Exploit vulnerability in code, Export data, Packet sniffer, Password dumper, Ram scraper, encrypt or seize stored data, Root-kit, Scan

network, Spam, Spyware, SQL injection, Utility, Worm, Unknown, and Other components) and Vector (Direct install, Download by malware, Email auto-execute, Email link, Email attachment, Instant messaging, Network propagation, Remote injection, Removable media, Web drive-by, Web download, Unknown, and Other components) families), Hacking (Variety (Abuse of functionality, Brute force, Buffer overflow, Cache poisoning, Session prediction, Cross-site request forgery, Cross-site scripting, Cryptanalysis, Denial of service, Foot-printing, Forced browsing, Format string attack, Fuzz testing, HTTP request smuggling, HTTP request splitting, HTTP response smuggling, HTTP Response Splitting Integer overflows, LDAP injection, Mail command injection, Man-in-the-middle attack, Null byte injection, Offline cracking, OS commanding, Path traversal, Remote file inclusion, Reverse engineering, Routing detour, Session fixation, Session replay, Soap array abuse, Special element injection, SQL injection, SSI injection, URL redirector abuse, Backdoor or Control and Command, Stolen authentication credentials, XML attribute blow-up, XML entity expansion, XML external entities, XML injection, XPath injection, XQuery injection, Unknown, and Other components), and Vector (3rd party desktop, Backdoor or command and control, Desktop sharing, Physical access, Remote shell, VPN, Web application, Unknown, and Other components) families), Social (Variety (Planting infected media, Bribery, Elicitation, Extortion or blackmail, Forgery, Influence tactics, Scam, Any type of *ishing, Pretexting, Propaganda, Spam, Unknown, and Other components), Vector (Documents, Email, In-person, Instant messaging, Phone, Removable media, Texting, Social media, Software, Website, Unknown, and Other components), and Target (Auditor, Call centre staff, Cashier or waiter, Customer, End-user or regular employee, Executive or upper management, Finance or accounting staff, Former employee, Helpdesk, Human resources staff, Maintenance, Manager, Partner, Guard, Software Developer, System or network administrator, Unknown, and Other components) families), Misuse (Variety (Knowledge abuse, Privilege abuse, Embezzlement, skimming, and related fraud, Data mishandling, Email misuse, Network misuse, Storage or distribution of illicit content, Unapproved workaround, Unapproved hardware, Unapproved software, Unknown, and Other components), and Vector (Physical access, LAN access, Remote access, Non-corporate, Unknown, and Other components) families), Physical (Variety (Assault, Sabotage, Snooping, Surveillance, Tampering, Theft, Wiretapping, Unknown, and Other components), Vector (Privileged access, Visitor privileges, Bypassed controls, Disabled controls, Uncontrolled location, Unknown, and other components), and Location (Partner facility, Partner vehicle, Personal residence, Personal vehicle, Public facility, Public vehicle, Victim secure area, Victim work area, Victim public area, Victim grounds, Unknown, and Other components) families), Error (Variety (Classification error, Data entry error, Disposal error, Gaffe, Loss, Maintenance error, Misconfiguration, Misdelivery, Misinformation, Omission, Physical accidents, Capacity shortage, Programming error, Publishing error, Malfunction, Unknown, and Other components), and Vector (Random error, Carelessness, Inadequate personnel, Inadequate processes, Inadequate technology, Unknown, and Other components) families), and Environmental (Deterioration, Earthquake, Electromagnetic interference, Electrostatic discharge, Temperature, Fire, Flood, Hazardous material, Humidity, Hurricane, Ice and snow, Landslide, Lightning, Meteorite, Particulates matter, Pathogen, Power failure, Tornado, Tsunami, Vermin, Volcano, Water leak, Wind, Unknown, and Other families).

Breached Asset Attributes - The breached asset classes are Server (Authentication, Backup, Database, DHCP, Directory, Distributed control system, DNS, File, Log or event management, Mail, Mainframe, Payment switch or gateway, POS controller, Print, Proxy, Remote access, SCADA system, Web application, and Other families), Network(Access control reader, Camera or surveillance system, Firewall, Hardware security module, IDS or IPs, Mobile broadband network, Private branch exchange, Private WAN, Programmable logic controller, Public WAN, Remote terminal unit, Router or switch, Storage area network, Telephone, VoIP adapter, Wired LAN, Wireless LAN, and Other families), User Devices(Authentication token or device, Automated Teller Machine, Desktop or workstation, Detached PIN pad or card reader, Gas “pay-at-the-pump” terminal, Laptop, Media player or recorder, Mobile phone or smart phone, Peripheral, POS terminal, Self-service kiosk, Tablet, Telephone, VoIP phone, and Other families), Media(Backup tapes, Disk media, Documents, Flash drive or card, Hard disk drive, Identity smart card, Payment card, and Other families), People(Administrator, Auditor, Call centre, Cashier, Customer, Developer, End-user, Executive, Finance, Former employee, Guard, Helpdesk, Human resources, Maintenance, Manager, Partner, and Other families), Unknown, and Ownership (personal (Yes or No components), Hosting (Yes or No components), and Management (Yes or No components) families).

Breached Content Attributes - The Breached Content classes are Confidentiality or Possession (Data disclosure (Yes, Potentially, No, and Unknown components), Data Variety (Authentication credentials, Bank account data, Classified, Copyrighted, Medical, Payment card data, Personal or identifying information, Sensitive internal data, System

information, Trade secrets, Unknown, and Other components), and Data State (Stored, Stored encrypted, Stored unencrypted, Transmitted, Transmitted encrypted, Transmitted unencrypted, Processed, and Unknown components) families), Integrity or Authentication (Created account, Hardware tampering, Influence or alter human behaviour, Fraudulent transaction, Log tampering, Misappropriation, Misrepresentation, Modified configuration, Modified privileges, Modified data, Software installation or code modification, Unknown, and Other families), and Availability or Utility (Destruction, Loss, Interruption, Performance degradation, Acceleration, Obscuration, Unknown, and Other families).
VERIS includes other entities such as Impact Assessment, Response, and Compromise. Impact Assessment attributes classes are Overall rating (Insignificant, Distracting, Painful, Damaging, Catastrophic, and Unknown families), Loss variety (Asset and fraud, Brand and market damage, Business disruption, Operating, Legal and regulatory, Competitive advantage, and Response and recovery families) and Loss rating (None, Minor, Moderate, Major, and Unknown families)
(www.veriscommunity.net/doku.php?id=enumerations, 30/1/13).

4. Review and Evaluation of Breach Data Capture Frameworks

VERIS focused on the capture of security breach incidents in general and therefore provided for less of capture of breach data details (example is the classification of all data types regarding PII under Authentication credentials and Personal or identifying information Data Types, losing certain details). DatalossDB.org provides for capture of many details of breach data but omitted some, and its content structure could be improved. The others offer certain enlightenments that revealed and filled apparent gaps. It should be noted that VERIS, Open Security Foundation Breach Data Capture, and other frameworks discussed, were consolidated, focused, innovated and complemented by ingenuity to achieve the proposed. The intention is to make the proposed have the best of content structure, format, and functionality suited to breach data capture while fostering acceptability. Primary industry classification using North American Industry Classification System components moved by VERIS was adopted.
Breach data capture frameworks summary comparison regarding certain features is presented in Table 1.

5. Conclusion

The absence of a generally accepted framework for collecting and classifying data breach security incident information in a common language and structure, and uniform classification of organisation were addressed. Breach data capture frameworks vary one from the other. VERIS and Open Security Foundation Breach Data Capture frameworks are notable attempts and the others have made noteworthy contributions. The proposed supports the course for a common generally accepted breach data capture framework by consolidating, focusing, innovating and complementing by ingenuity the existing ones, maintaining largely the structure and nomenclature for acceptability.

A continued proper capturing and analysis of breach data, leading to application of complimentary informed and apt countermeasures, would ensure a safer computing environment and increase the collective knowledge of the security community. It will also prove helpful to the planning of security efforts. The model provides certain bases for designing and implementing effective breach data capture and reporting system. The proposed model of breach data capture and reporting system, and the breach data capture framework, are complimentary efforts toward improved countermeasures against information security breaches.

References

Acquisti, A., Friedman, A., and Telang, R.(2006). Is there a cost to privacy breaches? An event study. In Workshop on the Economics of Information Security, 2006

Adebayo, A. O. (2012). A Foundation for Breach Data Analysis. Journal of Information Engineering and Applications, Vol.2 No.4, pp 17-23.

Adebayo, A. O., Omotosho, O. J., and Adekunle, Y. A. (2012). Statistical Insight into Breach Data toward Improved Countermeasures. Journal of Information and Knowledge Management, Vol. 2, No. 8 pp 40-51.

Aitoro, J. (2007). Reports of federal security breaches double in four months. Government Executive.com, October

23, 2007, www.govexec.com/dailyfed/1007/102307;1.htm. Retrieved November 11, 2010

Culnan, M J, and Williams, C C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. MIS Quarterly December 2009, Vol. 33, Issue 4 (pp. 673-687)

Eichin, M and Rochlis, J. (1989). With Microscope and Tweezers: An analysis of the Internet virus of November 1998. 1989 IEEE Symposium on Research in Security and Privacy, www.mit.edu/people/eichin/virus/main.html. Visited November 15, 2010

Gordon, L A, Loeb, M P, and Sohail, T. (2010). "Market Value of Voluntary Disclosures Concerning Information Security." MIS quarterly Vol. 34, No. 3

Hasan, R., and Yurcik, W. (2006). A Statistical Analysis of Disclosed Storage Security Breaches. International Workshop on Storage Security and Survivability: in conjuction with 12th ACM Conference on Computer and Communications Security, October, 2006

Helbush, A. (2009). Phishing Attacks Still on the Rise. Where to Start Technology Solutions Blog, http://www.wtsci.com/2009/11/Phishing-attacks-still-on the rise/ Visited November 11, 2010

Keizer, G. (2010). Apple Smashes Patch Record with gigantic Update. Computer World.com/s/article/9196118/Apple_smashes_patch_record_with_gigantic_update. Visited November 5, 2010

Mahmood, M.A, Siponen, M, Straub, D, Rao, H.R, and Raghu, T.S. (2010). "Moving Toward Black Hat research in Information Systems Security: An Editorial Introduction to the Special Issue." MIS Quarterly Vol. 34 No 3. Pp 431-433/September 2010

Oates, B J. (2009). Researching Information Systems and Computing. London - SAGE Publications Ltd

Ryan, J C H, and Jefferson, T I. (2003). The Use, Misuse and Abuse of Statistics in Information Security Research. Proceedings of the 2003 ASEM National Conference, St. Louis, Missouri

Shostack, A and Stewart, A. (2009). The new approach to Information Security. Harlow, Essex – Pearson Education Ltd

Tehan, R. (2005). Personal Data Security Breaches: content and incident summaries. In Congressional research Service Report for Congress, December 16, 2005

Vaishnavi, V., and Kuechler, W. (2004). Design research in information systems. www.isworld.org/researchdesign/drisISworld.htm. Retrieved 15/6/2011.

Table 1 - Breach Data Capture Frameworks Summary Comparison

FRAMEWORK	Scope	Content Format	Content Structure	Content Functionality	Completeness /Exhaustivity	Simplicity	Fit for Purpose
Databreaches.net	Breach Blogs	Fair	Fair	Fair	No	Simple	Fair
DatalossDB	Breach Data Capture	Satisfactory	Satisfactory	Satisfactory	No	Simple	Satisfactory
Identity Theft Resource	Breach Data Capture	Fair	Fair	Fair	No	Simple	Fair
Infosecurityanalysis.com	Summary Breach Data Capture	Fair	Fair	Fair	No	Simple	Fair
Privacy Rights ClearingHo.	Breach Data Capture	Fair	Fair	Fair	No	Simple	Fair
VERIS	General Incident Data Capture	Very Good	Very Good	Good	No	Much Details	Good
Proposed	Breach Data Capture	Consolidates and expands others	Consolidates and expands others	Consolidates and expands others	Yes	Satisfactory	Well Focused

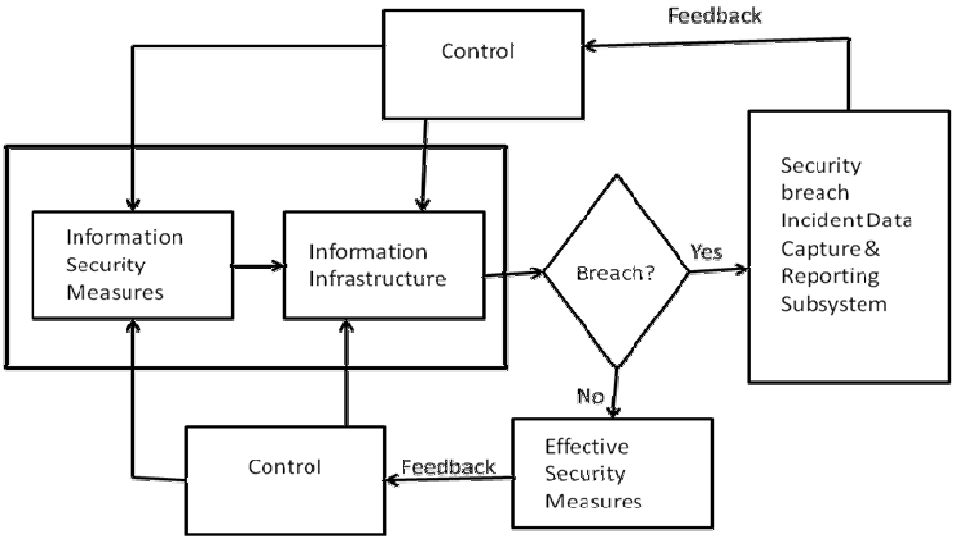

Figure 1 – Information Security Measure Flow System

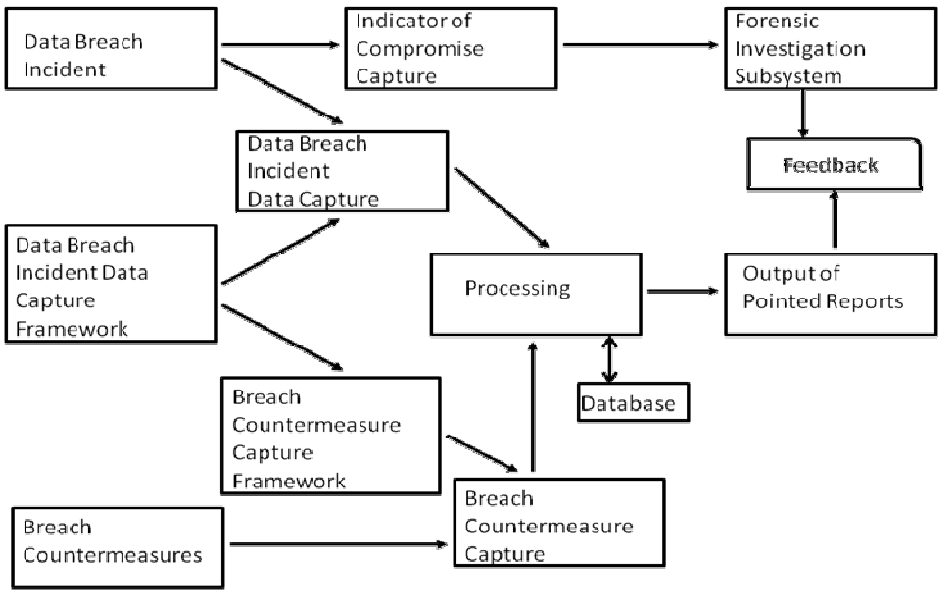

Figure 2 - Model of Security Breach Incident Data Capture and Reporting System

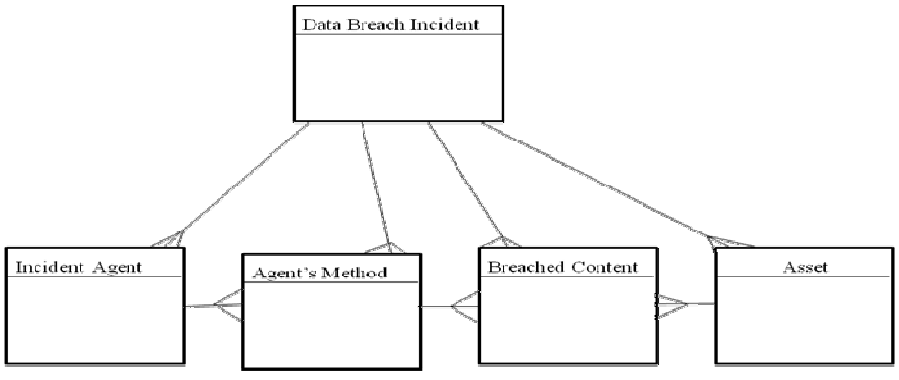

Figure 3 - The Relationships of the Basic Entities of an Incident

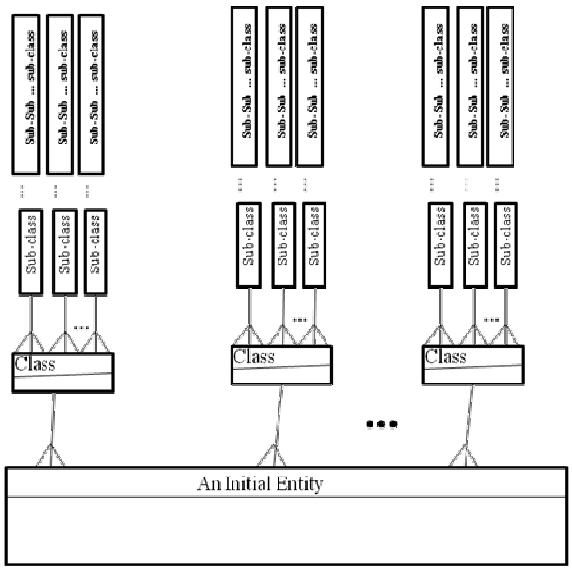

Figure 4 - Subsequent Relationships for any Initial Entity of an Incident

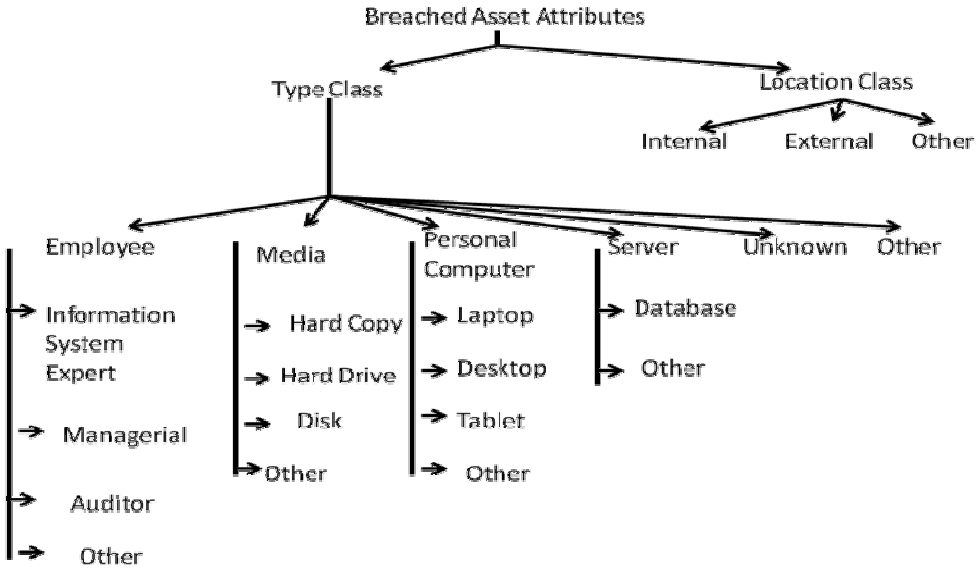

Figure 5: Breached Asset Attributes Depicted.

This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE's homepage: http://www.iiste.org

CALL FOR PAPERS

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. There's no deadline for submission. **Prospective authors of IISTE journals can find the submission instruction on the following page:** http://www.iiste.org/Journals/

The IISTE editorial team promises to the review and publish all the qualified submissions in a **fast** manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar