



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL **TEAM**

Raju Narayana Swamy (IAS) Indian Administrative Service **officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

diploma in Public

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

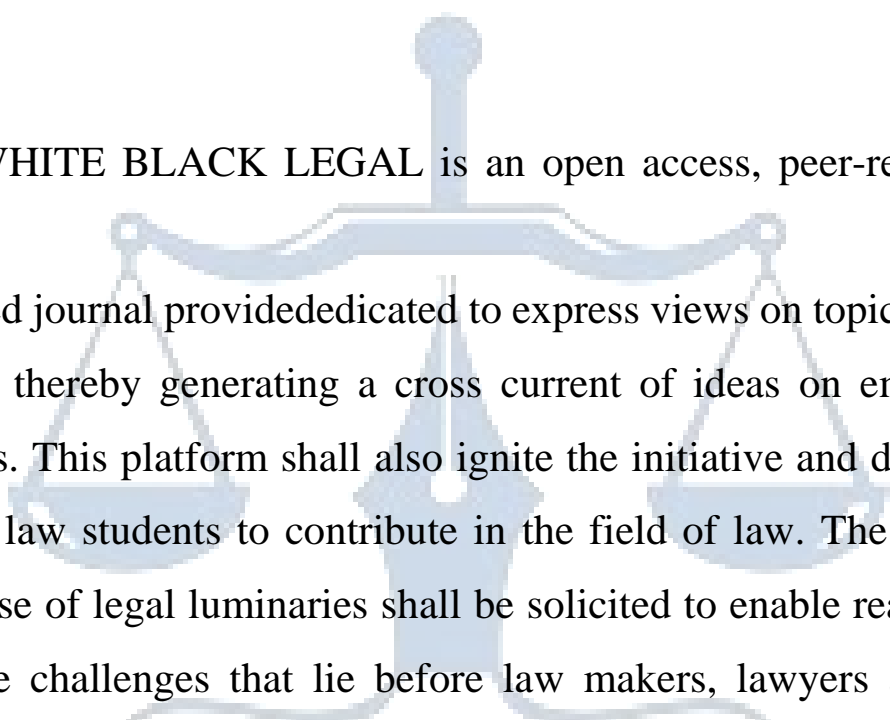


Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

CYBER FORENSIC TECHNIQUES FOR INVESTIGATING DATA BREACHES IN SOFTWARE DEVELOPERS AND IT SECTOR

AUTHORED BY - AMAN SHUKLA & PRERNA SINGH RAJPOOT

ABSTRACT:

Data breaches constitute an escalating and significant risk for software developers and the wider IT industry, as they reveal sensitive information, jeopardise personal and business security, and undermine trust in digital infrastructure. These breaches, from malicious assaults, insider threats, or system flaws, require comprehensive investigation to ascertain their core causes and avert future incidents. Cyber forensics is essential in this process, providing specialised methods to collect, preserve, and analyse digital evidence associated with data breaches. This research explores the use of sophisticated cyber forensic techniques to identify, examine, and resolve data breaches in the software development and IT sectors. The study seeks to establish a complete framework for discovering breach entry points, assessing damage degree, and implementing effective countermeasures by examining key methodologies like log analysis, network traffic monitoring, and data recovery. Furthermore, it underscores the significance of prompt breach identification and cooperation between forensic specialists and developers to mitigate operational and reputational damage. This research emphasises the necessity for ongoing training and integrating emerging forensic technologies to remain proactive against advancing cyber threats in these vital sectors.”

Keywords: Malicious assaults, Digital evidence, IT industry, Digital security

INTRODUCTION

The software development and IT industries are rapidly undergoing digital transformation, which has increased their attack surface and made them more susceptible to data breaches. These intrusions expose confidential data, imperil individual and corporate safety, and diminish confidence in digital infrastructure. A new survey states that the average cost of a data breach worldwide has increased to \$4.24 million, with the IT and software development sectors being among the most often attacked businesses.

Data breaches can occur owing to several circumstances, including intentional assaults, insider threats, system weaknesses, and human mistakes. Because of the intricacy and seriousness of these breaches, it takes specialist investigative methods to find the underlying reasons, minimise the harm, and stop such instances in the future.

Cyber forensics, an essential part of incident response, offers the know-how needed to gather, store, and examine digital evidence related to data breaches. Through the use of cutting-edge cyber forensic methods, investigators can:

1. Identify breach entrance sites and vectors
2. Determine the breadth and severity of the breach
3. Retrieve hacked data;
4. Examine network traffic and system logs;
5. Create workable countermeasures

This project intends to explore the applicability of cyber forensic techniques in analysing data breaches across the software development and IT sectors. By exploring key techniques, difficulties, and best practices, this study strives to provide a complete framework for increasing the resilience of these vital businesses against data breaches.

Additionally, in order to strengthen these industries' resilience against data breaches, this study will look into the best practices that these organisations might implement. Through an examination of actual case studies, this study will demonstrate the efficacy of diverse forensic methodologies and demonstrate how prompt and efficient breach investigations can mitigate harm, safeguard confidential data, and uphold confidence. The significance of incorporating cyber forensics into more comprehensive security plans will be emphasised, along with the need for cooperation between developers, IT specialists, and forensic specialists to guarantee a comprehensive strategy for data breach response and prevention.

In the end, this research will provide an all-encompassing framework that will assist companies in the IT and software development sectors in strengthening their entire cybersecurity posture in addition to handling data breaches. The objective of this study is to enhance the security and resilience of the digital ecosystem by offering practical insights into forensic methodology, breach investigation, and mitigation strategies.

LITRATURE REVIEW

1. *"Digital Evidence and Computer Crime" by Eoghan Casey (2011)*¹ - is a fundamental text in the field of digital forensics, providing a complete and authoritative guide to examining and interpreting digital evidence. This third version of the book, which was released in 2011, has grown to be a standard for law enforcement organisations and experts in digital forensics globally. Casey's experience shines through in his clear and simple explanation of complicated technical subjects, making the book accessible to both technical and non-technical readers. The full digital forensic process—from gathering and preserving evidence to analysing and presenting it—is covered in the text. Expert testimony, network investigations, digital evidence types, forensic analysis tools, email and mobile device forensics, and more are important subjects. The book's emphasis on practical application—which is exemplified by case studies and real-world examples that highlight important ideas—is among its strongest points. Casey also examines the moral and legal issues related to digital evidence, making sure that investigators are aware of the consequences of their work. The book was published in 2011, and while certain technical details may have changed since then, the underlying ideas and techniques are still applicable. The fast growth of digital technologies underlines the necessity for continual education and training in digital forensics.
2. *"Virtualization Security" by Dave Shackleford*² - is a detailed reference that digs into the subtleties of safeguarding virtualized systems, which have become important in modern IT infrastructures. Published in 2017, the book examines the particular security concerns offered by virtualization technologies, offering a deep assessment of both theoretical concepts and practical applications. Shackleford thoroughly investigates several virtualization technologies, highlighting the need for effective security measures throughout the virtualization lifecycle, from planning and deployment to maintenance and incident response. The author underlines the need for a tiered security approach, combining best practices for managing hypervisors, safeguarding virtual machines, and assuring data integrity. Additionally, Shackleford gives useful insights into compliance considerations and the developing threat landscape, making the book a vital resource for IT professionals, security practitioners, and enterprises wishing to

¹ Digital Evidence and Computer Crime. (2011). In Academic Press (Third Edition) [Forensic Science, Computers and the Internet; E-book: PDF]. Academic Press. https://booksite.elsevier.com/samplechapters/9780123742681/Front_Matter.pdf

² Shackleford, D. (2012). Virtualization Security: Protecting Virtualized Environments. Germany: Wiley.

defend their virtual environments efficiently. Through its blend of expert knowledge and effective techniques, "Virtualization Security" gives readers with the tools essential to negotiate the challenges of safeguarding virtualized infrastructures in an increasingly digital environment.

3. *"Penetration Testing: A Survival Guide"* by Halton, Weaver, Ansari, Kotipalli, and Imran³ is a comprehensive handbook that provides a structured approach to penetration testing. Published in 2017 by Packt Publishing, this book is an invaluable resource for IT professionals, security enthusiasts, and penetration testers. The authors, seasoned experts in the field, offer a practical guide that covers fundamental concepts, methodologies, and tools. One of the book's greatest strengths is its practical approach, focusing on real-world scenarios that make it an excellent resource for hands-on learning. The well-organized content progresses logically from basics to advanced topics, covering popular penetration testing tools such as Nmap, Metasploit, and Burp Suite. Real-world case studies illustrate key concepts and testing methodologies, further enhancing the book's value. However, some areas, such as web application testing, could benefit from more in-depth coverage. Additionally, cloud-specific penetration testing is not extensively explored. Given the rapidly evolving nature of cybersecurity, some information may become outdated. Despite these limitations, the book remains a vital resource for understanding penetration testing principles and methodologies. The target audience includes IT professionals, security enthusiasts, penetration testers, and cybersecurity students. This book is an excellent choice for those seeking practical guidance on penetration testing. While it may not cover every niche topic, it provides a solid foundation for further exploration..
4. *"Software Security: Building Security In"* by Gary McGraw (2006)⁴ presents a comprehensive analysis of the vital relevance of integrating security into the software development process. This book stands out as a crucial resource for developers, security experts, and organizational leaders who are eager to expand their understanding of software security and establish robust practices within their teams. The book covers a wide range of subjects, including threat modeling, secure coding methods, and testing methodologies. McKinnon emphasizes the necessity of collaboration between

³ Halton, W., Weaver, B., Ansari, J. A., Kotipalli, S. R., Imran, M. A. (2017). *Penetration Testing: A Survival Guide*. United Kingdom: Packt Publishing.

⁴Software Security Google Books
https://books.google.co.in/books/about/Software_Security.html?id=HCQdybpZXgC

development and security teams, building a culture of shared accountability that is crucial for creating secure software. The inclusion of real-world examples and case studies further emphasises the costs of security failures and highlights the benefits of proactive security measures. Additionally, the book tackles current trends and technologies, ensuring that readers are able to confront the growing landscape of software security concerns. McKinnon also gives real tools and resources that practitioners may employ to examine their present processes and execute any modifications.

STATEMENT OF PROBLEM

1. Data breaches in the software development and IT sector pose significant threats to sensitive information, business operations, and customer trust.
2. Despite growing awareness and investment in cybersecurity, often due to inadequate investigation and mitigation strategies.
3. The complexity of modern software systems and networks compounds the challenge, making it difficult to identify breach entry points and prevent incidents.

HYPOTHESIS

Employing advanced cyber forensic techniques can significantly improve the effectiveness of data breach investigations and mitigation strategies in software development and IT sectors.

RESEARCH QUESTION

1. What are the most common types of data breaches affecting software development and IT sectors?
2. What cyber forensic techniques are currently used to investigate data breaches in these sectors?
3. How effective are advanced cyber forensic techniques in identifying breach entry points and containing damage?

RESEARCH OBJECTIVES

1. Examine the current landscape of data breaches in software development and IT sectors
2. Investigate cyber forensic techniques for breach investigation and analysis
3. Identify key challenges and limitations in a breach investigation

SCOPE AND LIMITATION

This research's scope includes looking at data breaches that occur in the software development and IT industries, with an emphasis on cyber forensic methods for breach analysis and mitigation. The research will look at data recovery methods, network traffic monitoring, log analysis, and the difficulties and constraints associated with breach investigation. The study's dependency on existing literature and expert opinions may induce biases, while technical difficulties and resource limits may limit in-depth research.

Data Breach Investigation Techniques

2.1 Network traffic analysis and log analysis

Two essential methods in cyber forensics for looking into data breaches are network traffic analysis and log analysis. Investigators can identify abnormalities, track down unauthorised access, and identify the origins of security problems with the use of these techniques.

The main objective of network traffic analysis is to track and analyse the data packets that are transferred over a network. By studying traffic patterns, cyber forensic professionals can uncover odd activities such as unexpected data transfers, connections with malicious IP addresses, or aberrant bandwidth utilisation. This technique assists in locating possible points of entry for breaches, figuring out how data was exfiltrated, and determining whether the attacker is still using the system. Hackers utilise tools like Wireshark and Intrusion Detection Systems (IDS) to gather and examine network data in order to identify attack vectors and the command-and-control communications they use.

Another essential forensic method is log analysis, which is the methodical examination of logs produced by different systems, such as servers, firewalls, and applications. Investigators can follow an attacker's path thanks to logs, which offer comprehensive recordings of events including user logins, system modifications, and file access. Through the correlation of log data across several systems, forensic investigators can recreate the history of a breach, detect questionable user behaviour, and discover compromised credentials. Log analysis solutions like Splunk or ELK Stack automate the process, helping to analyse enormous datasets and find anomalies rapidly.

Together, network traffic and log analysis provide a holistic perspective of a data breach,

helping investigators assess the scale of the attack, correct vulnerabilities, and avoid repeat attacks. These strategies are critical for uncovering sophisticated attacks and guaranteeing system integrity in the aftermath of a breach.

2.2 Memory and disk forensics

Important methods in cyber forensics for looking into data breaches involving malicious software are malware analysis and reverse engineering. These technologies allow forensic professionals to understand how malware acts, identify its intent and devise countermeasures to limit its consequences.

Examining malicious software to comprehend its actions, capabilities, and effects on the infected system is known as malware analysis. Two categories of analysis exist: static and dynamic. With static analysis, investigators examine the file structure, strings, and signatures of the malware without running it in order to identify patterns that are known to be present in malware. Critical information can be extracted with the aid of programs like Binwalk or IDA Pro. Alternatively, dynamic analysis runs the malware in a sandbox or other controlled environment so that real-time actions can be seen. This procedure makes the malware's interactions with the system, the files it creates or alters, and if it connects with outside servers, all transparent. To locate payloads, such as ransomware or tools for data exfiltration, dynamic analysis is essential.⁵

Malware analysis is advanced by reverse engineering, which breaks down the malware's code to reveal its fundamental workings. This approach allows forensic professionals to determine how the malware was developed, its origin, and its attack vector. Dissecting complex malware that uses obfuscation tactics to avoid detection is much easier with the help of reverse engineering. Through code analysis, researchers can find hidden features, embedded attacks, and encryption techniques intended to spread throughout a network. In reverse engineering, tools like Ghidra and Radare2 are frequently employed.

By combining malware research and reverse engineering, cyber forensic professionals can expose the full breadth of a malicious assault, establish personalised detection methods, and prevent future data breaches by fixing vulnerabilities used by the infection.⁶

⁵ <http://www.porcupine.org/forensics/forensic-discovery/>

⁶ DRFWS 2005 Forensic Challenge. (n.d.).

2.3 Malware analysis and reverse engineering

Reverse engineering and malware analysis are essential cyber forensics techniques that help investigators recognise, lessen, and eliminate the consequences of malicious software following a data breach.

The practice of looking into malware to ascertain its actions, intentions, and effects is known as malware analysis. The two categories of analysis are static and dynamic. Static analysis is the process of examining the malware's code without running it. Investigators may frequently find signatures that correspond to well-known malware kinds by examining the signature's structure, strings, and libraries. To analyse the code and identify potential weak points or attack strategies, programs like Binary Ninja and IDA Pro are employed. Running the virus in a sandbox or virtual system allows you to see how it behaves in real-time, which is necessary for dynamic analysis. This technique reveals the files that the malware accesses or changes, how it communicates with the system, and whether it attempts to establish a connection with distant servers in order to conduct command-and-control or exfiltration of data.⁷

By breaking down malware's code to comprehend its underlying structure and operation, reverse engineering elevates malware analysis above its current state. This is especially crucial for advanced malware that conceals its actual purpose through encryption or obfuscation. The strategies and techniques that the malware uses to take advantage of security flaws in the system are made clear through reverse engineering. By using tools such as Ghidra or Radare2, investigators can reverse engineer malware and find malicious code that has been custom-built or has never been seen before. Along with generating patches for vulnerabilities that have been exploited, this approach aids in the creation of signatures for upcoming detection.⁸

Finding out how a breach happened, determining the extent of the attack, and putting in place effective defences all depend on reverse engineering and malware research. Understanding the workings of the virus and strengthening systems against similar attacks are two ways that these tactics assist organisations in preventing future intrusions.

<https://web.archive.org/web/20061007145847/http://www.dfrws.org/2005/challenge/>

⁷ LiveKd for Virtual Machine Debugging - Mark's Blog - Site Home - TechNet Blogs. (2010, October 14). <https://web.archive.org/web/20101018201303/http://blogs.technet.com/b/markrussinovich/archive/2010/10/14/3360991.aspx>

⁸ Sengupta, S. (2023, April 22). Reverse Engineering Malware: Techniques And Tools For Analyzing And Dissecting Malicious Software. Medium. <https://sudip-says-hi.medium.com/reverse-engineering-malware-techniques-and-tools-for-analyzing-and-dissecting-malicious-software-4dd5949135f0>

2.4 Cloud computing and virtualization investigations

Virtualisation and cloud computing are becoming essential components of contemporary IT architecture, but they also provide new difficulties for data breach investigators. The dynamic, distributed nature of cloud infrastructures demands specialized forensic approaches to discover, analyse, and mitigate intrusions efficiently.

Cloud Computing Forensics involves evaluating data stored on remote servers, often scattered across numerous locations. Specialised obstacles that investigators have to deal with include multi-tenancy—where several clients share the same infrastructure—data ownership concerns, and no physical access to servers. Typically, cloud forensic investigations use the cloud service provider's (CSP) logs for analysis. These logs capture critical events including access history, file updates, and API queries, letting investigators reconstruct the timeframe and tactics of a breach. Collecting log data unique to a cloud is made easier by tools like Azure Monitor and AWS CloudTrail. Virtual machine (VM) backups and snapshots are another common tool used by investigators to find proof of lost or compromised data.

The field of virtualisation forensics is devoted to the examination of security lapses in virtualised systems, including hypervisors and virtual machines (VMs). Since numerous VMs can run on a same physical computer, attackers may exploit flaws in one VM to obtain access to others, known as a "VM escape." To determine the extent of the assault, data extraction from the infected virtual machine and the hypervisor is necessary for virtualisation forensics. To find evidence of malware or unauthorised access, memory dumps of virtual instances are analysed using forensic tools like Redline and Volatility.

Since data may exist in various places, maintaining chain of custody and handling encrypted communications and storage provide significant issues for both cloud and virtualisation forensics professionals. In order to gather and evaluate evidence for these investigations without compromising service availability, cloud service providers must work with us and specialised technologies must be used.⁹

Investigators can evaluate data intrusion, locate breach entry points, and assist enterprises in

⁹ Brandao, P. R. (2019). Forensics and Digital Criminal Investigation Challenges in Cloud Computing and Virtualization. American Journal of Networks and Communications, 8(1), 23. <https://doi.org/10.11648/j.ajnc.20190801.13>

strengthening security in remote systems by utilising forensic techniques unique to cloud and virtualisation.

Software Development and IT Sector-Specific Investigations

3.1 Investigating data breaches in software development environments

Investigating data breaches in software development environments involves particular issues due to complex systems and networks, collaborative development approaches, and the use of open-source elements and third-party libraries. These environments necessitate specific investigative techniques that take into account elements like third-party components, collaboration tools, source code analysis, and development environment configuration.

Researchers should locate compromised systems and points of entry, gather and examine logs from version control and development tools, perform code reviews to find malicious modifications or backdoors, and speak with stakeholders and the development team in order to conduct a thorough investigation of a breach. To fully comprehend the breach, analysis of system call records and network traffic is also necessary.

Collaboration tool audits for platforms like Slack and Jira, code analysis platforms like Code Dx and Veracode, Git forensics tools like GitLog and GitFS, and network traffic analysis tools like Wireshark and Tcpdump are just a few of the tools and approaches that can help with these investigations.

Even with these tools and methods, investigators still have to contend with issues including intricate system design, quickly evolving development environments, little access to third-party components, and juggling research with continuing development work.

Best practices advise putting secure coding techniques and code reviews into practice, keeping an eye on network traffic and development environment logs, regularly assessing vulnerabilities, and creating incident response plans specifically designed for software development environments in order to address these issues. Investigators can efficiently manage the complexity of software development systems to find breach reasons, contain damage, and stop similar events by using these tactics.

3.2 Secure coding practices and vulnerabilities

Data breaches in the IT industry are frequently caused by software code flaws that hackers use to access private data. Cyber forensics plays a critical role in finding these gaps, tracing the breach, and understanding how coding faults contributed to the compromise. To stop breaches, it is imperative for software developers to use safe coding techniques. This entails incorporating security into the entire software development lifecycle, validating and sanitising input, handling errors appropriately and logging them, storing and transmitting data securely, and doing routine code reviews and testing.

These security measures may not completely prevent coding vulnerabilities such as buffer overflows, SQL injection, and cross-site scripting (XSS). Cyber forensic investigators examine source code and point out coding errors that attackers might have exploited using tools like dynamic testing tools (like Burp Suite) and static code analysers (like SonarQube). Forensics experts can establish how malicious inputs or payloads were created to influence the software by looking at the susceptible code.¹⁰

An essential part of breach investigations is vulnerability analysis. IT specialists and software engineers need to be able to spot misconfigured and unpatched software, recognise exploits such as privilege escalation and remote code execution (RCE), and examine error messages, logs, and access controls. Vulnerability scanners, like Nessus and OpenVAS, assist in identifying vulnerabilities. After finding coding vulnerabilities, investigators make recommendations to repair holes, develop secure coding practices, and conduct frequent code reviews and testing.

Secure coding standards, frequent security training, and ongoing testing and monitoring should be top priorities for IT workers and software developers to prevent intrusions. They can reduce the likelihood of a breach, bolster defences, and safeguard sensitive data by doing this. In the IT industry, protecting software integrity and averting data breaches require the use of cyber forensics and safe coding techniques.¹¹

¹⁰ Snyk. (2020, December 21). Secure coding practices every developer should know. <https://snyk.io/learn/secure-coding-practices/>

¹¹ OWASP Secure Coding Practices-Quick Reference Guide | OWASP Foundation. (n.d.). <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>

Collaboration between software developers, IT specialists, and cyber forensic specialists is necessary for effective breach investigations. They may find weaknesses, stop breaches, and put strong security measures in place by cooperating to stop similar occurrences in the future. Proactive vulnerability analysis and secure coding strategies are essential in the constantly changing world of cyber threats to safeguard confidential data and preserve software system integrity.

3.3 Insider threat investigations in IT sector

Insider threats pose a serious challenge to the IT industry since workers, contractors, and other trusted individuals may misuse their access to compromise confidential data, cause disruptions to business operations, or harm their reputations. Because of the frequent legitimate access that insiders have to systems and data, insider threats are harder to identify than external ones. Investigating these occurrences, locating malevolent insiders, and halting additional harm all depend heavily on cyber forensics.

Insider threats come in different forms. These include malevolent insiders who steal or compromise data on purpose, careless workers who inadvertently lead to breaches due to subpar security procedures, and compromised insiders whose credentials have been obtained by outside attackers. A thorough understanding of the networks, access restrictions, and IT systems in use is necessary to investigate such threats.

An essential part of any inquiry into insider threats is log and access monitoring. Forensic specialists can identify odd patterns of behaviour, including unauthorised data transfers, strange login timings, or attempts to access files that are banned, by examining system and access logs. Logs from several systems can be gathered and correlated with the aid of SIEM (Security Information and Event Management) platforms like Splunk or LogRhythm in order to identify potentially suspicious activity. A thorough log analysis can show whether a worker changed important files, accessed data without permission, or used the network in an unexpected way. Behavioral Analysis is also useful in insider threat investigations. In order to identify departures from typical behaviour, forensic investigators frequently examine user behaviour and digital footprints. This involves keeping an eye on data transfer rates, file download activity, and correspondence with other parties. An effort at data exfiltration, for instance, can be indicated by a rise in data transfers prior to an employee's retirement.

Securing digital evidence, including as emails, file access logs, and network activity, is necessary for forensic data collection in order to track insider behaviour and ascertain intent. By studying this data, forensic teams can establish a timeline of events, proving malevolent intent or finding negligent conduct.

3.4 Cloud and Virtualization Security

Although virtualisation and cloud computing have completely changed the IT industry, they also present new security risks. Investigating security breaches in these contexts takes particular skills. Difficulties in conducting cloud security investigations include data fragmentation among many cloud services, restricted access to cloud infrastructure, intricate access control and authentication, and reliance on cloud provider monitoring and logging.

Investigations into virtualisation security also provide unique challenges. Investigation procedures are made more difficult by dynamic virtual machine (VM) environments, hypervisor vulnerabilities, virtual machine (VM) escape strategies, and complicated network segmentation and isolation. Investigators use a variety of methods to get over these obstacles, such as memory and disc forensic analysis, virtualisation platform log and configuration review, network traffic analysis, packet capture, cloud provider log and monitoring analysis, and hypervisor and virtual machine introspection.

Investigations into cloud and virtualisation security are made easier by a number of techniques and technologies. Virtualisation security technologies like VMware vCloud and Cloud Security Gateways like CloudLock offer crucial visibility and control. Log analysis and security threat identification are aided by SIEM and log management tools like Splunk. Forensic analysis tools, such as Volatility and EnCase, aid in studying memory and disk data.¹²

Organisations should build incident response plans specifically designed for these environments, use encryption and secure data storage, monitor network traffic and logs, regularly conduct vulnerability assessments, and implement strong access controls and authentication to ensure effective cloud and virtualisation security. Cloud provider liability and shared responsibility, virtualisation platform vulnerabilities, network segmentation and

¹² Kundan, A. P. (2018). VMware Cross-Cloud Architecture: Automate and orchestrate your Software-Defined Data Center on AWS. Packt Publishing Ltd.

isolation, data sovereignty and compliance, and incident response and containment tactics are important factors to take into account.

Through comprehension of the intricacies involved in cloud and virtualisation security enquiries, establishments may enhance their readiness and reaction to security incidents, safeguarding confidential information and preserving the authenticity of their IT framework.

Advanced Topics and Emerging Trends

4.1 Artificial intelligence and machine learning in cyber forensics

A paradigm shift in the field of cyber forensics has been sparked by the integration of artificial intelligence (AI) and machine learning (ML). By employing AI-driven forensic analysis tools, investigators may investigate massive volumes of data with greater efficiency and accuracy. While natural language processing retrieves relevant information from logs and documents, deep learning algorithms may analyse network traffic to detect harmful behaviour. Algorithms for grouping and clustering data classify and organise information, enabling a deeper analysis. Training machine learning models on large-scale datasets makes it possible to identify unknown malware and zero-day exploits, trace data exfiltration, reconstruct attack timelines, and identify affected accounts. Automatic forensic reporting and visualisation, predictive analytics for threat hunting, and intelligent incident response systems are some of the emerging developments in AI-powered cyber forensics.¹³

Cyber forensics can reap numerous advantages from incorporating AI and ML. Improved efficiency and accuracy lead to fewer false positives and shorter investigation times by improving threat detection and response. Nonetheless, there are still issues with data quality and bias, interpretability and explainability of the model, and interaction with current forensic tools.

Network intrusion detection systems driven by machine learning, intelligent digital forensic analysis platforms, and malware analysis and sandboxing are examples of real-world uses of AI-powered cyber forensics. With the ongoing development of AI and ML technologies, cyber forensics will become more automated, freeing up investigators to concentrate on strategic

¹³ Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International Digital Investigation*, 48, 301675. <https://doi.org/10.1016/j.fsidi.2023.301675>

decision-making and advanced analysis.

It's critical to handle the difficulties and constraints associated with AI-powered cyber forensics in order to guarantee accurate and successful investigation results. The main goals of future research should be to improve data quality, build reliable AI and ML models, and improve model interpretability. Cyber forensics can then use AI and ML to their fullest extent in order to counteract increasingly complex cyberthreats.

4.2 Blockchain and cryptocurrency investigations

With the introduction of blockchain technology and the growth of cryptocurrencies, cyber forensics has changed dramatically in recent years. The decentralised and unchangeable nature of blockchain presents distinct possibilities and obstacles for forensic enquiries. Investigators can track transactions in real time thanks to its transparency, which is very helpful when looking into illegal activity like fraud, ransomware attacks, and money laundering. However, the anonymity given by cryptocurrency can hamper these investigations. To de-anonymize users and connect bitcoin addresses to real-world identities, forensic specialists use a variety of instruments and methods, such as blockchain analysis software.

The significance of international cooperation is further underscored by emerging trends in cyber forensics, since cryptocurrencies frequently function outside of established financial institutions and legal frameworks. The legal complications surrounding digital currencies are causing governments to contend with differing laws and regulations, necessitating forensic teams to modify their methodology in order to comply. Further adding to the complexity is the growing integration of decentralised finance (DeFi) systems with smart contracts. Comprehending the workings of these technologies is essential for investigators to properly analyse and evaluate the related data.¹⁴

Moreover, the methods employed by cybercriminals also advance with blockchain technology. Cyber forensics has a new frontier as privacy coins, which improve user anonymity, come into being. These days, investigators have to be up to date with the latest developments, which

¹⁴ Investigations, B. (2024, August 27). Blockchain Intelligence Group | Crypto Investigations and Risk Management. Blockchain Intelligence Group. <https://blockchaingroup.io/#:~:text=Blockchain%20Intelligence%20Group%20powers%20intelligence,former%20U.S.%20Federal%20and%20experts.>

means they need to continue learning and honing their specialised abilities in blockchain forensics. In the end, the convergence of cryptocurrency and blockchain investigations highlights the necessity of a proactive and flexible approach in cyber forensics, guaranteeing that law enforcement and administrative agencies can successfully tackle the obstacles presented by this quickly evolving field.¹⁵

4.3 Internet of Things (IoT) forensics

The Internet of Things' (IoT) growth has changed the field of cyber forensics, posing opportunities as well as difficulties for investigators. IoT devices, ranging from smart household appliances to industrial sensors, regularly generate large volumes of data, which can be essential in forensic investigations. The variety and decentralised structure of these devices, however, make data collection and processing more difficult. Since every Internet of Things device could use a different protocol and have a distinct data storage system, forensic specialists must create specialised techniques for every kind of device.

The necessity for specific tools and methods to gather, store, and examine data from these devices is at the centre of emerging developments in IoT forensics. The use of methods like cloud forensics, which stores data on multiple Internet of Things devices, and remote acquisition, which allows data to be obtained from a device over a network, is growing among forensic investigators. This calls for in-depth knowledge of the several communication protocols and security methods used by diverse manufacturers.¹⁶

Additionally, the difficulty of assuring data integrity and authenticity is crucial, as IoT devices are typically prone to tampering and hacks. Ensuring a correct chain of custody for the obtained data is crucial, especially in legal circumstances. A further trend in IoT forensics is the incorporation of artificial intelligence and machine learning, which help investigators spot patterns suggestive of malicious activity and automate data processing.

Having strong IoT forensic frameworks is becoming more and more important as the IoT ecosystem grows. To create standards and best practices, stakeholders from the manufacturing,

¹⁵ Gonzalez, S. (2022, October 24). What is a Cryptocurrency Investigation? - ERMPProtect Cybersecurity. ERMPProtect Cybersecurity - Cybersecurity | Digital Forensics | Penetration Testing. <https://ermprotect.com/blog/what-is-a-cryptocurrency-investigation/>

¹⁶ Al-Masri, E. (2020). Internet of Things (IoT) Forensic Science. In Springer eBooks (pp. 1–8). https://doi.org/10.1007/978-3-319-32903-1_352-1

law enforcement, and cybersecurity industries must work together. By addressing these difficulties head-on, the discipline of IoT forensics can boost its efficiency in preventing cybercrime and assuring digital responsibility in the age of connectivity.

Case Studies & Best Practices

5.1 Real-world data breach Investigation case studies

Case studies from actual data breaches are valuable educational resources for cyber forensics professionals by showcasing cutting-edge techniques and best practices. Approximately 147 million people's personal information was compromised in the 2017 Equifax data breach, which is one prominent example. The investigation uncovered several flaws in security procedures and response tactics, and the intrusion was linked to a vulnerability in a web application framework. The attackers were eventually identified by forensic investigators using network analysis and log examination to track the breach's origins. This scenario underlines the significance of maintaining a current inventory of assets, strict patch management, and having a clearly defined incident response plan.¹⁷

Target's 2013 data breach, which resulted in the credit card details of over 40 million consumers being compromised, is another noteworthy instance. The incident, which underscores the dangers connected to supply chain vulnerabilities, happened after hackers obtained access through a third-party vendor. The results of the forensic investigation showed that malware was utilised by the attackers to obtain credit card information at the point of sale. Target's response entailed a thorough investigation of the malware and its transmission mechanisms, allowing the company to upgrade its security procedures. This event brought home how important it is to manage vendor risk and deploy cutting-edge security measures like network segmentation and intrusion detection systems.¹⁸

One more recent instance is the 2020 cyberattack known as SolarWinds, which targeted numerous government and commercial organisations in the United States using a sophisticated supply chain attack. Forensic experts evaluated the malware and the compromised systems to establish the attack vector and the degree of the breach. This incident made clear how crucial

¹⁷ Equifax Data Breach Settlement. (2024, July 24). Federal Trade Commission. <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>

¹⁸ Gavett, G. (2015, March 30). Could Target Have Prevented Its Security Breach? Harvard Business Review. <https://hbr.org/2014/03/could-target-have-prevented-its-security-breach>

it is to conduct ongoing monitoring and threat hunting in addition to working together with cybersecurity and law enforcement organisations to lessen the impact of breaches.¹⁹

These case studies show that cooperation between stakeholders, technological know-how, and strategic planning are all necessary for efficient data breach investigations. Organisations may create strong cybersecurity frameworks, strengthen incident response procedures, and promote a continuous improvement culture in their security operations by studying historical incidents.

5.2 Cyber Forensic Investigation Best Practices

Cyber forensic investigations play a critical role in identifying cybercrimes, protecting evidence, and reducing potential threats. Adopting industry best practices guarantees comprehensive, accurate, and legally sound investigations. Here are some essential best practices collected from several case studies:

1. **Create a Clearly Definable Incident Response Plan:** The cornerstone of any successful cyber forensic investigation is an incident response plan (IRP). It is important for organisations to set up procedures for locating, containing, and eliminating risks. To guarantee a coordinated reaction, the plan should specify roles, duties, and communication tactics.
2. **Preservation of Evidence:** It's critical to keep digital evidence intact. Forensic investigators must apply write-blocking techniques to prevent any change of data during gathering. For the evidence to be supported in court, the evidence gathering procedure must be properly documented, including the chain of custody documents.
3. **Utilize Advanced Forensic technologies:** Employing state-of-the-art forensic technologies boosts the ability to gather, analyze, and interpret digital evidence. Tools that can automate procedures and offer in-depth insights into the data include EnCase, FTK, and open-source programs like Autopsy.
4. **Train and Certify Staff:** To guarantee that forensic investigators are current with the newest techniques, instruments, and legal requirements, they undergo ongoing training and certification. Professional designations like Certified Information Systems Security Professional (CISSP) or Certified Computer Examiner (CCE) can improve reputation and knowledge.

¹⁹ Active Exploitation of SolarWinds Software | CISA. (2020, December 13). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software>

5. Perform Regular Security Audits: Vulnerability assessments and security audits on a regular basis can help find vulnerabilities before they are taken advantage of. Organisations can strengthen their defences and expedite subsequent investigations by testing security measures on a regular basis and changing them in light of findings.
6. Work in Partnership with Law Enforcement and Experts: Building connections with law enforcement and outside forensic specialists helps improve communication of information and the capacity to conduct investigations. Collaboration can also benefit in coping with jurisdictional problems and legal complications.
7. Concentrate on Reporting and Data Analysis: Forensic investigations depend heavily on accurate data analysis. Researchers must to prioritise not just the retrieval of data but also the interpretation and contextualisation of the results. Reports that are succinct and easy to read are crucial for sharing findings with management and legal teams, among other stakeholders.
8. Put Digital Hygiene Practices into Practice: Encouraging employees to practice digital hygiene can help to lower the likelihood of cyber problems. Regular training on phishing awareness, secure password procedures, and safe browsing helps decrease human error, which is often a key vector for breaches.

Organisations may enhance their cyber forensic skills and ensure a methodical investigation of incidents while safeguarding digital assets and upholding legal compliance by following these best practices. By emphasising prevention, readiness, and resilience in the face of changing cyberthreats, these approaches promote a proactive cybersecurity culture.²⁰

CONCLUSION AND SUGGESTION

Cyber forensic techniques are vital in detecting data breaches in the software development and IT business, and their integration should correspond with the current digital frameworks. It makes sense to use these strategies, which will strengthen the cybersecurity defences in place and improve investigative capacities by utilising international best practices. While applying cyber forensic techniques can present common concerns including prejudice and human sensitivity, these issues can be resolved. Potential dangers are highlighted by current rules and laws, but resolving these issues is essential for a successful integration. To traverse these hurdles, it's crucial to acknowledge the relevance of cyber forensics in analysing data breaches.

²⁰ Cybercrime Module 4 Key Issues: Standards and best practices for digital forensics. (n.d.). : <https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html>

Deleted file recovery, live analysis, cross-drive analysis, stochastic forensics, and reverse steganography are some of the key techniques. Software development and IT companies can improve cybersecurity, safeguard sensitive data, and guarantee the integrity of digital systems by adopting these strategies and resolving any obstacles. Eventually, for society to advance and a secure digital landscape to be promoted, cyber forensic techniques must be integrated into current frameworks.

BIBLIOGRAPHY

1. Digital Evidence and Computer Crime. (2011). In Academic Press (Third Edition) [Forensic Science, Computers and the Internet; E-book: PDF]. Academic Press. https://booksite.elsevier.com/samplechapters/9780123742681/Front_Matter.pdf
2. Shackleford, D. (2012). Virtualization Security: Protecting Virtualized Environments. Germany: Wiley.
3. Halton, W., Weaver, B., Ansari, J. A., Kotipalli, S. R., Imran, M. A. (2017). Penetration Testing: A Survival Guide. United Kingdom: Packt Publishing.



WHITE BLACK
LEGAL