EU General Data Protection Regulation Compliance Challenges for Cloud Users

Conference Paper · May 2019

CITATIONS
0

READS
34

1 author:

Bob Duncan
University of Aberdeen
55 PUBLICATIONS **350** CITATIONS

SEE PROFILE

EU General Data Protection Regulation Compliance Challenges for Cloud Users

Bob Duncan
Business School
University of Aberdeen, UK
Email: bobduncan@abdn.ac.uk

***Abstract*—The EU General Data Protection Regulation (GDPR) has been with us now since the 25th May 2018. It is certainly the case that in many of the 28 EU countries, regulators were not all properly resourced by the starting deadline. However, progress has been made since then. We review the challenges faced by cloud users, and consider whether all the compliance challenges existent then have persisted, and whether there are any other challenges that have evolved. We examine the most serious risks faced by cloud users and consider how users might mitigate their exposure to these hard problems. We provide a series of practical solutions which might help them to keep abreast with these issues while proper long term solutions can be found.**

Keywords–EU GDPR; Compliance; Cloud computing; cloud forensic problem; unresolved vulnerabilities.

I. INTRODUCTION

It is certainly the case that the new EU General Data Protection Regulation (GDPR) [1], has some serious teeth, with maximum fine levels for each breach being the greater of €20million or 4% of global turnover. It is also the case that a number of cloud vulnerabilities are still unresolved, and are frequently exploited by attackers. This results in a potential nightmare scenario for cloud users where they are unable to ensure compliance with the regulation. In May last year, 17 out of 24 regulators polled in a Reuters survey [**?**], claimed they would not be ready in time for the new regulation. However, in addition, other jurisdictions are now taking a lead from the EU to implement regulations or legislation of their own.

In the US, the State of California introduced their own version of the EU GDPR within a month of it going live [2]. Currently, the White House is working on introducing stringent data protection legislation based on the model of the EU GDPR. It is likely to be only a matter of time before other jurisdictions follow suit. For global corporates in particular, this is likely to present a serious challenge to their ability to demonstrate compliance with these regulations and other legislation. Make no mistake, there is no doubt that these regulators have a serious intent, and there is little doubt that they will exercise their considerable powers to bring unwilling cloud users into line.

We start by looking at the most serious challenges highlighted by two cloud security organisations — the Cloud Security Alliance (CSA) [3], and the Open Web Application Security Project (OWASP) [4]. The CSA were set up specifically to examine cloud security issues. The OWASP project was initially set up to examine Web based vulnerabilities, but over time extended their remit to incorporate mobile, internet of things and cloud vulnerabilities as well. Both organisations collect data on vulnerabilities and make good suggestions to help mitigate these issues. Both issue a report every three years which brings attention to their understanding of the most serious vulnerabilities.

Achieving information security is a big challenge already for all companies who use conventional distributed network systems, but once cloud systems are involved, the challenge increases exponentially. This mainly arises due to the complexity that the many issues of additional relationships and agendas of different participant companies involved brings to cloud ecosystems. Much research has been carried out to attempt to resolve these problems e.g., [5]–[14].

One of the most challenging, and as yet, still not properly unresolved issue is the cloud forensic problem [15]. Many are aware of it, but no-one seems to be prepared to discuss it, let along try to properly resolve the problem. It is of course a technical problem to address, but that does not mean it can be left unresolved. Regulators will quite rightly expect some mitigating steps be taken to address the issue, rather than allowing companies to trust to luck.

If any company using cloud is unable to resolve the cloud forensic problem, we suggest this will present such a fundamental issue that it will be impossible for that company to comply with this new regulation. As far back as 2011 and in subsequent years [16]–[22], a great deal of research was focussed on trying to resolve this issue, yet it is clear from looking at regulatory fines for breaches that the message is not getting though.

In 2012, Verizon estimated that a total of 174 million data records were compromised [23]. Yahoo disclosed a 1 billion compromised account breach in the 2013 attacks, yet when Verizon took over Yahoo two years ago, it turned out that **ALL 3 billion accounts** had been compromised [24]. By 2017, records compromised had increased to an estimated 2 billion records lost or compromised in the first half of 2017 alone [25]. In the last year, it is estimated by Gemalto in their Breach Level Index, that over 4.5 billion data records were lost or stolen in the first half of 2018 [26], an increase of 133% on the same period in 2017. The current level of data records lost is running at 6.4 million records per day [27], of which only 4% were encrypted. It is clear that data breaches are continuing at an alarming rate. Of particular concern is the 96% of unencrypted records compromised being exposed.

In Section II, we look at the top cloud vulnerabilities identified by both the CSA and OWASP. In Section III, we look at what the Cloud Forensic Problem is, and address why it is such a challenging problem to overcome. In Section IV, we address the minimum requirements necessary to achieve com-

pliance. In Section V, we look at whether this approach will ensure good security and privacy is possible. In Section VI, we consider future developments of this work, and in Section VII, we discuss our conclusions.

II. The Most Serious Cloud Vulnerabilities

We start by looking at the most recent vulnerability list for the CSA and OWASP. Their most recent list was published in 2017, and is based on the most damaging vulnerabilities for the 2016 year. We can see the comparison in the Tables below.

TABLE I: CSA TOP 12 CLOUD VULNERABILITIES 2017 [28]

Priority	CSA Top 12 Vulnerabilities
1	Data Breaches
2	Insufficient Identity, Credential and Access Management
3	Insecure Interfaces and APIs
4	System Vulnerabilities
5	Account Hijacking
6	Malicious Insiders
7	Advanced Persistent Threats
8	Data Loss
9	Insufficient Due Diligence
10	Abuse and Nefarious Use of Cloud Services
11	Denial of Service
12	Shared Technology Vulnerabilities

TABLE II: OWASP TOP 10 CLOUD VULNERABILITIES 2017 [29]

Priority	OWASP Top 10 Vulnerabilities
1	Accountability & Data Risk
2	User Identity Federation
3	Regulatory Compliance
4	Business Continuity & Resilience
5	User Privacy & Secondary Usage of Data
6	Service & Data Integration
7	Multi-Tenancy & Physical Security
8	Incidence Analysis & Forensics Risk
9	Infrastructure Security
10	Non-Production Environment Exposure

It is clear that each has taken a completely different approach to the perceived vulnerabilities, thus expanding the range of the most important vulnerabilities to a total of 22. In the case of the CSA, they have take the approach of identifying the 12 most important technical challenges faced by cloud users. On the other hand, OWASP have completely changed their approach by shifting to the Behaviour Driven Development (BDD) process, which shifts the focus away from technical issues alone to encompass all the stakeholders in cloud and in particular the business procedural oriented aspects. They further develop this by taking a risk-based approach, and have identified the 10 most dangerous risks facing cloud users.

While technical challenges are vitally important to address, it is equally important to address the risks which address mostly the non-technical element of cloud use. When we realise that the business architecture of a company comprises a combination of people, process and technology [30], and not technology alone, we can start to see how combining these two different approaches will have value. However, we have only considered two aspects of the foundational triad of business architecture. We must also consider the impact of people challenges.

People have long proved to be a serious security weakness in organisations. It is clear that criminals have long realised that the easiest way to successfully attack any system is through the weakest link — and that is invariably always people. We list here some 16 extremely successful social engineering attacks. We must add a proviso that these attacks are not specific to cloud users only, but they are common indeed. In fact, social engineering became the most successful attack vector in 2015 [31].

TABLE III: 16 SUCCESSFUL SOCIAL ENGINEERING ATTACKS ©2019 Duncan

Attack Name	Attack Description
Phishing	These are the most common type of attacks leveraging social engineering techniques. Attackers use emails, social media, instant messaging, and SMS to trick victims into providing sensitive information or visiting a malicious URL in an attempt to compromise their systems.
Watering Hole	A "watering hole" attack consists of injecting malicious code into the public Web pages of a site that the targets are known to visit. Once a victim visits the page on the compromised website a backdoor trojan is installed on their computer
Whaling Attack	This is an extension of a Phishing attack, used to steal confidential information,personal data, access credentials to restricted services/resources and specifically information with relevant value from an economic and commercial perspective. This is targeted at executives of private companies and government agencies, hence the use of whaling to describe the "big fish"
Pretexting	This term describes the practice of pretending to be someone else, such as an external IT services operator in order to obtain private information.
Baiting & Quid Pro Quo Attacks	Baiting exploits the user's curiosity, with the promise of some good that the attacker uses to deceive the victim, often with a malicious file disguised as a 'security' update. The Quid Pro Quo or 'something for nothing' attack offers a service or benefit to the victim in exchange for information, or facilitation of an attack
Tailgating	This is where an attacker gains physical entry to a restricted area in contravention of security policy by walking through behind an authorised person when they enter a secure area
Deceptive Phishing	Arises when attackers attempt to replicate a legitimate company email account to elicit information from the victim
Spear Phishing	These attacks are specially tailored for a single victim using knowledge obtained from social media profiles and other public sources of information, exposing the victim to identity theft, malware, credit card fraud and even blackmail
Whaling / CEO Fraud	In this attack, victims are asked to provide information or to authorise payment urgently at the behest of the CEO
Vishing	This is where an attack is perpetrated by Voice over IP (VoIP). Becasue the VoIP server can be made to look like anything, it can appear that the call is coming from an important outside entity such as a bank or the Inland Revenue
SMiSHing	This attack purports to come via SMS, and asks the victim to respond by clicking on a malicious link, or calling the attacker's phone, who then tries to extract information
W2 Phishing	This is where the attacker pretends to be a senior executive or an external service like the Inland Revenue in order to obtain personal information such as NI numbers
Pharming	This is more sophisticated than Phishing, whereby the attacker used cache poisoning to purport to come from an official web site.
Ransomware Phishing	This Phishing variant contains a link to download malware usually in the form of ransomware
Dropbox Phishing	This Phishing variant purports to come from Dropbox and seeks to obtain private files and photos usually leading to blackmail
Google Docs Phishing	This variant of Phishing spoofs the Google Docs login page and seeks to collect the victim's userid and password

These attacks are particularly well crafted and have proved to be exceptionally successful in tricking victims into giving up sensitive information, passwords and so on. Often, they look every bit as good as official communications, despite the fact that sometimes they are poorly constructed, or use poor English

grammar and spelling. While it is fair to say that the social engineering attacks equally relate to non-cloud environments, nevertheless, they still present a serious challenge to the cloud environment.

Now, we can see that it is clear that not only is the business architecture of any company comprised of a combination of people, process and technology, but so too are attacks crafted to attack each of these sectors.

III. The Cloud Forensic Problem (and Why it is Such a Hard Problem)

While all computing systems are constantly under attack, this can present a far more serious issue for users of cloud systems. Once an attacker gains a foothold in a cloud system and becomes an intruder, there is little to prevent the intruder from helping themselves to any amount of data, especially that which is covered by the GDPR, either by viewing it, modifying it, deleting it or ex-filtrating it from the victim system [32]–[34]. Worse, should the intruder gain sufficient privileges, they are then able to completely delete all trace of their incursion, perhaps deleting far more records than they need to in the process, leading to further problems for business continuity.

After the intruder has removed every trace of the intrusion, the forensic trail will have little left to follow, which means many companies will be totally unaware that the intrusion has taken place, let alone understand what records have been accessed, modified, deleted or stolen. This leads to a serious issue for companies who believe they have retained a full forensic trail in their running instance. They frequently fail to realise that without special measures being taken to save these records off-site [8], everything will vanish when the instance is shut down, often by the intruder. In such a case, there will be no mitigating factor that the company can use, rendering them liable to the full force of the penalties under the regulation.

In any cloud based system, there is a need to ensure a complete and intact audit trail is stored off cloud in order for the breached organisation to be able to tell which records have been accessed, modified, deleted or stolen. Otherwise, if the audit trail and all forensic records have been deleted, there will be no physical means for any organisation to be able to tell which records have been accessed, modified, deleted or stolen, putting these organisations immediately in multiple breaches of the GDPR. This will also pose a serious impediment to using business continuity plans for recovery.

Thus, in addition to the 38 attacks discussed in the previous section, we must now add this difficult challenge to the list.

IV. What do we Need to do to Achieve Compliance with the GDPR?

Simply address the above 39 points and we will be compliant, yes? Sadly, the reality is that those actions alone will not guarantee compliance, and we will explain the reason in the following subsections.

A. Cloud Security Alliance

It is not as simple as dealing with our 39 identified vulnerabilities. If we start with the CSA top 12 vulnerabilities, this represents just the 12 most damaging vulnerabilities. The CSA maintains a full list of all known cloud vulnerabilities, which is known as the Common Vulnerabilities and Exposures (CVE) list [35]. The list comprises all known vulnerabilities which are, or are expected to become public. The CVE Numbering Authority (CNA) [36], assigns all such identified CVEs with a unique number, which are then published in the MITRE CVE database [37]. Workarounds and fixes, as they are developed, are associated with the appropriate CVE number.

This list also feeds the National Vulnerability Database (NVD) [38], which was launched by the National Institute of Standards and Technology (NIST) [39], in 2005. NIST provide a range of enhanced information about each vulnerability including such information as fix information, severity scores and impact ratings. The NVD also offers this information by Operating System (OS); by vendor name; product name, and/or version number; as well as by vulnerability type, severity, related exploit range and impact. NIST also offer the Common Vulnerability Scoring System (CVSS) [40]. The first version, released in 2005, following feedback was updated to V2 in 2007, and following further feedback was updated to V3 in 2015.

The following website provides a list of 12 free online tools to test your website to scan for website security vulnerabilities and malware.

TABLE IV: 12 FREE TEST SITES FOR CSA VULNERABILITIES [41]

No	Site Address
1	Scan My Server
2	Sucuri
3	Qualys SSL Labs, Qualys FreeScan
4	Quttera
5	Detectify
6	SiteGuarding
7	Web Inspector
8	Acunetix
9	Netsparker Cloud
10	UpGuard Web Scan
11	Tinfoil Security
12	Observatory

B. The Open Web Application Security Project

Likewise for the OWASP issues. These represent only the top 10 issues. OWASP also provide suggestions to address or mitigate each issue.

There is also another organisation, WAVSEC [42], who have compiled a list of 51 companies who provide both proprietary and open access tools to test your website for OWASP and other vulnerabilities.

C. Social Engineering

Since social engineering attacks are attacks on people, there are no software tools available to test for the presence of such attacks on any system, making the job of defence rather more challenging. It is therefore necessary to ensure that companies keep on top of the ever increasing range of new attacks being developed, so that proper training can be made available for every single employee in the company. It will also be important to ensure that adequate training is provided to ensure that actors who are not employees of the company, such as suppliers, customers and others are made aware of the dangers surrounding these attacks. Additional security provisions and monitoring may be necessary to ensure a higher level of protection is available.

D. The Cloud Forensic Problem

We have seen that to do nothing would not be a viable option as far as GDPR compliance is concerned. Attacks will continue unabated. We must therefore be prepared and armed with whatever tools we can develop to ensure we achieve as high a level of compliance as we possibly can. For a pragmatic approach to helping resolve this problem Duncan and Whittington [43], make some practical suggestions to mitigate this potential problem.

We therefore need to consider what the absolute minimum technical requirement might be to attain our objective of GDPR compliance. We know that under the GDPR the organisation must be able to:

- provide a Right of Access (under Article 15) to personal data by data subject, if requested;
- provide the means to comply with a Right to Erasure (under Article 17) by data subject, subject to the appropriate grounds being met;
- provide privacy by design;
- in the event of a data breach, report the breach to the Supervisory Authority within 72 hours after having become aware of the data breach (Article 33). The breach must also be reported to the controller without undue delay after becoming aware of a personal data breach;
- in the event of a data breach, notify the data subject if adverse impact is determined (under Article 34), unless the data was encrypted;

To meet the first requirement, we must ensure the provenance and veracity of the contents of the database. For the second requirement, if appropriate, the same provision would apply.

For the third requirement, the cloud system must be designed in accordance with the recommendations of the Article 29 Working Party [44], which suggests the reports produced by ENISA should be followed. This report [45], specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. Furthermore, it specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys. ENISA have also produced a stream of other relevant reports, including a Cloud Risk report in 2009 [46], and recommendations for certification in 2017 [47].

For the fourth requirement, we would require to ensure the provenance and veracity of the contents of the database. For the fifth requirement, where the data is not yet encrypted, the same provision would also apply. However, it should be stressed that it will always be preferable to ensure data is encrypted before it leaves the control of the data owner.

It is clear that where no steps have been taken to ensure the cloud forensic problem has been mitigated, the organisation will fail on every count. Thus, as a minimum, we need to ensure the following steps are taken:

- all personal data should be encrypted, and this should be performed locally;
- the encryption and decryption keys should not be maintained on the cloud instance;
- a full audit trail of the entire database must be maintained off-site;
- full forensic records of all users having accessed the database and carried out any commands on the database must be collected and stored off-site.

V. Will this Approach Provide Good Security and Privacy?

The business architecture of a company comprises a combination of people, process and technology [30], not technology alone. As we have seen in Section III, all three aspects of the business architecture are subject to attack. We saw how social engineering attacks in Table III, could be used effectively against people in the business. From the OWASP weaknesses list in Table II, we see how effectively processes can be attacked, and from the technical attacks in Table I, how a wide range of effective attacks can be perpetrated agains the technological systems of the company.

We must, of course, understand that we cannot simply address each of the three areas in isolation, but must instead be prepared to consider the possibility that an attack could end up compromising the company more easily through combining attacks from two or more of the three sectors to develop an even more effective attack.

Thus, we must take a multi-pronged approach to keeping our cloud systems secure:

- People
  - Keep abreast of evolving social engineering attacks
  - Train the people in the organisation regularly to recognise these attacks and deal with them properly
- Process
  - All processes must be properly documented and kept up to date
  - All processes must be checked for potential vulnerabilities
- Technology
  - Test continually for vulnerabilities
  - Monitor constantly
  - Analyse logs regularly
  - Constantly review for new evolving vulnerabilities and exploits
- Cloud Forensic Problem
  - Encrypt all data
  - Ensure data is backed up off-cloud
  - Ensure encryption/decryption keys are stored off-cloud

In addition, we should regularly check all systems to ensure no new vulnerabilities or weaknesses have appeared. We should regularly check for evolving threats and take appropriate mitigatory action. We should perform continuous monitoring and analytics on all systems to ensure they are as up to date and secure as possible. Adding an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) would also be a prudent measure to take.

There are two essential tasks that must be performed to ensure the effectiveness of this approach. Persistent storage in the running cloud instance cannot retain data beyond its currently running lifetime [8], so we need to ensure that all necessary logs and data is stored securely elsewhere. Also, since the default settings for the majority of all database software involves logging being turned off by default [32], it is essential that we turn it on in all running cloud instances, with the data being stored securely elsewhere.

All of these measures will give us a much higher chance of achieving a good level of security and privacy, as well as the means to deliver a compliant system from the point of legislative and regulatory requirements.

VI. Future Work

We need to understand what data we require to keep. To meet our legislative and regulatory compliance requirements, we need to understand the 5 W's — namely: Who is accessing our system? Where have they come from? What are they looking for? When is this happening? From this data, we should be able to infer the Why? Are they authorised to be in the system, to enter the system the way they have, to look at the data they are trying to access, and at the time they are trying to access it? Deducing the Why can give an indicator of anomalous behaviour.

We plan to construct a working model based on the ideas outlined in this paper with which to test this solution over the next 6 months, which will allow us to confirm how well it might work in the real world. It is not overly complicated to be able to do this, which means even the smallest business would have the means to ensure proper compliance can be achieved.

VII. Conclusion

As each of the EU countries gets their regulators properly in place and responding to breaches, and as their expertise starts to grow, there is no doubt that the level of fines will start to grow.

Once serious fines start to be levied, it is likely that many companies will start to get the message, and will finally wake up to the seriousness of this particular regulation. The forthcoming GDPR fines will certainly get some serious attention. In this paper, we have considered whether it is possible to achieve regulatory compliance where any organisation is using cloud computing. It is clear that without suitable precautions being put in place, the answer is a resounding "No!".

We have outlined the key requirements from the GDPR to which all organisations falling under its jurisdiction must comply. We have identified the currently unresolved "Cloud Forensic Problem" as presenting the largest obstacle to achieving compliance. We have proposed how this challenging problem may be approached to ensure that cloud users can be fully compliant with this new regulation, with little more than being sensibly organised. Clearly, additional cost will require to be incurred, and there may be a small impact on latency, but these costs could significantly mitigate the possibility of a huge regulatory fine in the event of a breach. It is also likely that this approach will ensure faster discovery of the occurrence of a breach, thus minimising the potential impact on business continuity.

References

[1] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ [Retrieved: March 2019]

[2] Reuters, European Regulators, 2018. [Online]. Available: https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X. [Retrieved: March 2019]

[3] California, "The California Consumer Privacy Act of 2018." [Online]. Available: https://www.caprivacy.org/ [Retrieved: March 2019]

[4] CSA, "Cloud Security Alliance," 2019. [Online]. Available: https://cloudsecurityalliance.org/ [Retrieved: March 2019]

[5] OWASP, "Open Web Application Security Project," 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP_Cloud_Security_Project [Retrieved: March 2019]

[6] M. Felici, "Cyber Security and Privacy: Trust in the Digital World and Cyber Security and Privacy EU Forum 2013 Brussels, Belgium, April 18-19, 2013 Revised Selected Papers," in Commun. Comput. Inf. Sci. Springer International Publishing, 2013, vol. 182 CCIS, pp. 77–88.

[7] Y. Y. Haimes, B. M. Horowitz, Z. Guo, E. Andrijcic, and J. Bogdanor, "Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems," Syst. Eng., vol. 18, no. 3, 2015, pp. 284–299.

[8] C. Millard, I. Walden, and W. K. Hon, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2," Leg. Stud., vol. 27, no. 77, 2012, pp. 1–31.

[9] R. K. L. Ko, P. et al., "TrustCloud: A framework for accountability and trust in cloud computing," Proc. - 2011 IEEE World Congr. Serv. Serv. 2011, 2011, pp. 584–588.

[10] R. K. L. Ko, B. S. Lee, and S. Pearson, "Towards achieving accountability, auditability and trust in cloud computing," Commun. Comput. Inf. Sci., vol. 193 CCIS, no. PART 4, 2011, pp. 432–444.

[11] N. Papanikolaou, S. Pearson, and M. C. Mont, "Towards Natural-Language Understanding and Automated Enforcement of Privacy Rules and Regulations in the Cloud: Survey and Bibliography," Analysis, 2011, pp. 1–9. [Online]. Available: http://www.springerlink.com/index/T63266U4407458T5.pdf [Retrieved: March 2019]

[12] S. Pearson, "Taking account of privacy when designing cloud computing services," Proc. 2009 ICSE Work. Softw. Eng. Challenges Cloud Comput. CLOUD 2009, 2009, pp. 44–52.

[13] S. Pearson, "Towards Accountability in the Cloud," IEEE Internet Comput., vol. 15, no. 4, jul 2011, pp. 64–69.

[14] D. Pym and M. Sadler, "Information Stewardship in Cloud Computing," Int. J. Serv. Sci. Manag. Eng. Technol., vol. 1, no. 1, 2010, pp. 50–67.

[15] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, "Ontological Approach toward Cybersecurity in Cloud Computing Categories and Subject Descriptors," in Sci. Technol., 2010, pp. 100–109.

[16] B. Duncan, M. Whittington, and V. Chang, "Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult," in Proc. 2017 Int. Conf. Eng. Technol. ICET 2017, vol. 2018-Janua, 2018.

[17] K.-K. Choo and A. Dehghantanha, "Contemporary Digital Forensics Investigations of Cloud and Mobile Applications," in Contemp. Digit. Forensic Investig. Cloud Mob. Appl. Elsevier, 2017, pp. 1–6.

[18] N. Papanikolaou, S. Pearson, M. C. Mont, and R. Ko, "A Toolkit for Automating Compliance in Cloud Computing Services," Int. J. Cloud Comput., vol. x, no. x, 2014, pp. 45–68.

[19] K. Ruan, J. James, J. Carthy, and T. Kechadi, "Key terms for service level agreements to support cloud forensics," in IFIP Adv. Inf. Commun. Technol., 2012, vol. 383 AICT, pp. 201–212.

[20] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," Digit. Investig., vol. 10, no. 1, 2013, pp. 34–43.

[21] J. Singh and J. M. Bacon, "On middleware for emerging health services," J. Internet Serv. Appl., vol. 5, no. 1, 2014, p. 6.

[22] J. Singh, J. Bacon, and D. Eyers, "Policy Enforcement Within Emerging Distributed, Event-based Systems," Proc. 8th ACM Int. Conf. Distrib. Event-Based Syst. - DEBS '14, 2014, pp. 246–255.

[23] J. Singh, J. Powles, T. Pasquier, and J. Bacon, "Data Flow Management and Compliance in Cloud Computing," Cloud Comput., no. Special Issue on Legal Clouds., 2015, pp. 1–12.

[24] Verizon, "2012 Data Breach Investigations Report," Verizon, Tech. Rep., 2012. [Online]. Available: https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf [Retrieved:March 2019]

[25] S. Khandelwal, "Its 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach," 2017. [Online]. Available: https://thehackernews.com/2017/10/yahoo-email-hacked.html [Retrieved: March 2019]

[26] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017.

[27] GDPR.Report, "Gemalto Breach Level Index data records lost or stolen in the first half of 2018," 2018. [Online]. Available: https://gdpr.report/news/2018/10/09/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018/ [Retrieved: March 2019]

[28] Gemalto, "Data Breach Statistics," 2019. [Online]. Available: https://breachlevelindex.com/ [Retrieved: March 2019]

[29] CSA, "CSA Top 12 Cloud Vulnerabilities," Tech. Rep., 2017.

[30] OWASP, "OWASP Top 10 Web Application Security Risks for 2017," 2017. [Online]. Available: https://https//www.owasp.org/index.php/Top_10-2017_Top_10 [Retrieved: March 2019]

[31] PWC, "UK Information Security Breaches Survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com www.bis.gov.uk [Retrieved: March 2019]

[32] W. Ashford, "Social engineering confirmed as top information security threat in 2015," 2015. [Online]. Available: https://www.computerweekly.com/news/4500273577/Social-engineering-confirmed-as-top-information-security-threat [Retrieved: March 2019]

[33] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization, no. April. Rome: IEEE, 2016, pp. 125–130.

[34] G. Weir, A. Aßmuth, M. Whittington, and B. Duncan, "Cloud Accounting Systems, the Audit Trail, Forensics and the EU GDPR: How Hard Can It Be?" in Br. Account. Financ. Assoc. Scottish Area Gr. Annu. Conf.relax Aberdeen: BAFA, 2017, p. 6.

[35] P. Tobin, M. McKeever, J. Blackledge, M. Whittington, and B. Duncan, "UK Financial Institutions Stand to Lose Billions in GDPR Fines: How can They Mitigate This?" in Br. Account. Financ. Assoc. Scottish Area Gr. Annu. Conf., BAFA, Ed., Aberdeen, 2017, p. 6.

[36] CSA, "Common Vulnerability and Exposure List," 2018. [Online]. Available: https://cve.mitre.org/cve/ [Retrieved: March 2019]

[37] CSA, "CVE Numbering Authorities," 2019. [Online]. Available: https://cve.mitre.org/cve/cna.html [Retrieved: March 2019]

[38] Mitre, "CVE Database," 2019. [Online]. Available: https://cve.mitre.org/ [Retrieved: March 2019]

[39] NIST, "National Vulnerability Database," 2019. [Online]. Available: https://nvd.nist.gov/ [Retrieved: March 2019]

[40] NIST, "NAtional Institute of Standards and Technology," 2019. [Online]. Available: https://www.nist.gov/ [Retrieved: March 2019]

[41] NIST, "Common Vulnerability Scoring System (CVSS)," 2019. [Online]. Available: https://www.nist.gov/publications/common-vulnerability-scoring-system-cvss

[42] C. Kumar, "12 Online Free Tools to Scan Website Security Vulnerabilities & Malware," 2019. [Online]. Available: https://geekflare.com/online-scan-website-security-vulnerabilities/ [Retrieved: March 2019]

[43] WAVSEC, "Evaluation of Web Application Vulnerability Scanners in Modern Pentest/SSDLC Usage Scenarios," 2018. [Online]. Available: http://sectooladdict.blogspot.com/ [Retrieved: March 2019]

[44] B. Duncan and M. Whittington, "The Complexities of Auditing and Securing Systems in the Cloud is there a Solution and will the GDPR move it up the Corporate Agenda?" Int. J. Adv. Secur., vol. 11, no. 3&4, 2018, pp. 232–242.

[45] D. M. Thompson, D. B. Ligon, J. C. Patton, and M. Pape, "Effects of life-history requirements on the distribution of a threatened reptile," 2017. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF [Retrieved: March 2019]

[46] ENISA, "Article 4 Technical Report," ENISA, Tech. Rep., 2011.

[47] ENISA, "Cloud Risk," ENISA, Tech. Rep., 2009. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment [Retrieved: March 2019]

[48] ENISA, "Recommendations on European Data Protection Certification," Tech. Rep., 2017.