Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis

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

***Abstract*—Many attackers constantly threaten the very survival of all organisations. They will attack any and every IT component of every organisation, whether financial, industrial, retail, service, educational, charitable or governmental, using whatever means they can to breach these systems. They ignore legislation, regulations and standards, do not care who they inconvenience, or hurt. They have no moral scruples and will have no compunction about attacking the weakest link in any organisation — the people. Why is this a problem? The answer is the European Union General Data Protection Regulation, which is effective from 25th May, 2018. The new regulator will have the power to impose fines for non-compliance to the maximum of €20 million or 4% of the previous year's global turnover. Jurisdiction for organisations requiring to be compliant is now global and these organisations are obliged by regulation to report any breach within 72 hours of discovery, potentially leading to massive fines. In this paper, we highlight the need for all such organisations to be aware of the serious pitfalls they face when considering the impact of this regulation should they fail to be compliant. We make some sensible suggestions for actions that organisations might take to mitigate their risk now. We also outline our plans for a test study to determine how effective our suggestions might be.**

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

I. INTRODUCTION

It is certainly the case that all organisations, no matter the market sector, whether public or private, business or charitable, governmental or non government organisations, large or small, are all at risk from the sustained capability of attackers to attempt to breach their systems. We can liken this to a myriad sharks swimming relentlessly around the IT resources of orgnisations, doing their best to live well from what they can scavenge by breaching their IT systems. Of these, Carcharodon Carcharias, the Great White Shark is considered the apex predator of the shark world.

Information security presents a huge challenge for companies who use conventional distributed network systems [1], but for those who use cloud, the challenge increases exponentially [2]–[6]. There are a multiplicity of relationships to consider in the use of cloud systems, with a great many different actors who will have access to an organisation's systems and data. Each may have differing agendas. The technology is complex as are the relationships between the actors.

The new European Union (EU) General Data Protection Regulation (GDPR) [7] will likely present one of the greatest compliance challenges faced by organisations, not just in this country, but across the globe. Again, the magnitude of the challenge increases significantly for cloud users.

However, when we consider this regulation in some greater detail, we can see that the regulators will have some serious power behind them. The amount of power the EU GDPR Regulator will hold is what prompts us to describe their position as Carcharodon Carcharias Moderator Europa Universalis — since there is the potential for exercising this power to raise potentially limitless fines across the globe. In the event of a serious data breach, the regulator can find up to the greater of €20 million or 4% of global turnover based on the previous year's accounts — for every single breach. At least Carcharodon Carcharias has a natural limit following a feeding frenzy, after which it becomes more or less harmless until the food is digested. Carcharodon Carcharias Moderator Europa Universalis will have no such natural limit.

There are many who ask why, in the light of Brexit, should the UK concern themselves with the EU GDPR? There are two responses to that question. The first is that the UK government have announced that after Brexit, the UK would include this regulation under UK legislation [8], and would take a much more robust approach to the rights of the individual. The second is that all organisations anywhere in the globe who hold any Personally Identifiable Information (PII) pertaining to any resident anywhere in the EU will be subject to EU jurisdiction in this regulation. A great many existing UK organisations already hold such PII. There will be no escape from it.

In Section II, we identify what the Cloud Forensic Problem is, how it can impact on conventional distributed systems and consider why it is such a challenging problem to overcome. In Section III, we look at the GDPR background and related work, and in Section IV, we take a look at the minimum requirements for compliance for any company that falls under the jurisdiction of the forthcoming EU GDPR. In Section V, we ask whether it is possible to achieve Compliance with the EU GDPR without addressing the Cloud Forensic Problem. In Section VI, we make some sensible suggestions that companies might carry out to mitigate the effects of the GDPR, and in Section VII, we outline the specification of hardware and software we will use for the pilot study we will run later this year,

including both cloud and distributed network infrastructure. In Section VIII, we address what our pilot study will seek to achieve. In Section IX, we consider the limitations of this work, along with a short discussion and in Section X, we discuss our conclusions.

II. The Cloud Forensic Problem (and Why it is Such a Difficult Problem)

Six years ago, Verizon estimated that a total of 174 million data records were compromised [9]. At that time, the global average time between breach and discovery was 6 months. Last year this had increased to an estimated 2 billion records lost or compromised in only the first half of 2017 [10]. Yet the global average time between breach and discovery was still in the order of 4 weeks.

The longer an intruder remains in any system, the more damage they can do, including the deletion of the forensic trail which could be used by forensic scientists to understand who penetrated the system, how they got in and what they accessed. With conventional distributed systems, there is still a chance that a good forensic scientist will be able to recover sufficient snippets of forensic information to have some idea of what has been going on. Unfortunately, with all cloud systems, there is nothing to prevent the intruder from completely deleting all this data, including the whole cloud running instance if they wish. This represents the Cloud Forensic Problem.

Yahoo eventually disclosed a 1 billion compromised account breach in the multiple 2013 cyber attacks, yet when Verizon took over Yahoo last year, their investigation discovered that all 3 billion accounts had been compromised [11]. Clearly, the longer an intruder remains within a system undetected, the more dangerous they become.

In order to comply with the GDPR, it is necessary for organisations to report a breach within 72 hours of discovery, and part of that reporting involves an understanding of which records have been accessed, modified, deleted or ex-filtrated from the system. Clearly, the cloud forensic problem can make this an impossible discovery for cloud, and where the intruder is skilled and has had sufficient time inside a conventional distributed system, it is likely that the same result will follow.

III. GDPR Background and Related Work

The EU GDPR has been a long time in the making. Early research mostly centred around the legal profession. In 2010, Weber [12], in writing about potential privacy issues concerning data protection, observed that no such regulation yet existed. A couple of years later, Kuner [13] wrote about the fact that the EU were to bring out such legislation. Costa and Poullet [14] commented on the fact that the legislation was to be brought in as a regulation, rather than a directive, meaning it would go straight into effect when the time came, rather than having to be passed by all EU member states. Ruberstein [15] questioned whether big data would herald the end of privacy, or would be a new beginning.

Mantelero [16] compares the 'right to be forgotten' in the new Regulation against previous privacy legislation, both in the EU and the US, and notes the improvement in protection levels. Ambrose and Ausloos [17] argue over the finer points of such rights, and conclude the 'right to erasure' in the EU regulation should not be confused with the 'right to oblivion' in the US legislation. Koops [18] observes that the three main points of the EU regulation are based on fallacies, namely that the regulation can give data subjects control over their data, that reform simplifies the law and that data protection law should be comprehensive. The author argues that in all three cases, the reality is the opposite of what has been claimed.

By 2015, we start to see input from other disciplines with more technical input. Bartolini et al., [19] point out the level of vagueness in the regulation, both from a legal and a technical standpoint. Luger et al., [20] also express concern about the lack of precision in the wording of the regulation. In 2016, Safari [21] believes the new regulation will set a new global standard for personal data protection. Buttarelli [22] argues that the regulation represents the best means of ensuring the development of a new gold standard for data protection.

By 2017, general interest in the GDPR is starting to pick up. Maldof [23] makes the point that many companies who will have to comply with the regulation will need to adapt their approach to a risk based approach, and approach with which many are unfamiliar. Zerlang [24] believes the regulation could lead to a milestone in the convergence of cyber-security and compliance. Duncan and Whittington [25] propose a simple means of safeguarding against both the cloud forensic problem to aid compliance with the GDPR. Duncan [26] makes some pragmatic suggestions on how to deal with GDPR compliance.

IV. The Minimum Requirements for Compliance with the EU General Data Protection Regulation

For the absolute minimum technical requirement to achieve GDPR compliance, the organisation must be able to:

- Provide a Right of Access (under Article 15) to personal data if requested by the data subject;
- Provide the Right to Erasure (under Article 17) by a data subject who qualifies for this request;
- 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 comply with a Right of Access, and a Right to Erasure we need to ensure the veracity of the contents of the database. In the case of Privacy by Design, a cloud system must be designed in accordance with the recommendations of the Article 29 Working Party [27], which suggests the reports produced by ENISA should be followed. This report [28] 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 a practical and relatively safe way of ensuring privacy, as long as only the data owner, not the cloud service, holds the decryption keys. ENISA have also published a range of other useful and relevant reports, including a Cloud Risk report in 2009 [29],

and well as sensible recommendations for certification in 2017 [30]. Obviously, the same approach should also be taken for conventional distributed systems.

In the case of a data breach, we must be sure of the veracity of the contents of the database. Some good research has been carried out into data provenance [31]–[34]. Where the data is not yet encrypted, the same provisions would also apply. However, it will always be preferable to ensure all PII data is encrypted before it leaves the control of the data owner.

As soon as all trace of the intrusion has been deleted, there will be little forensic trail left to follow, meaning many companies will be completely unaware that the intrusion has even taken place. As to understanding what records have been accessed, modified, deleted or stolen, they will have no chance. Companies often believe they have retained a full forensic trail in their running instance, but often forget that without special measures being taken to save these records off-site [2], they will vanish when the instance is shut down. And with escalated privileges, there is nothing to stop the intruder from taking this destructive step.

In a cloud system where these steps have not been taken, compliance will fail on all counts, leading to increased fine levels. In a distributed system where an intruder is allowed to remain for extended periods of time, it is likely that the same outcome will apply. Thus, we must ensure the following steps are taken [35]:

- All PII data should be encrypted locally;
- The encryption and decryption keys should not be maintained on any cloud instance;
- A full audit trail of the entire database must be maintained off-site;
- Full forensic records of all users accessing the database and commands used on the database must be collected and stored off-site.

V. Is it possible to achieve Compliance with the EU GDPR without addressing the Cloud Forensic Problem?

It is clear that it will not be possible to achieve this objective, whether using cloud or not. Clearly, looking at recent security breach reports [10], [36]–[43], a great many organisations still have difficulty in identifying when they have been breached. The fact that they are being breached year after year is certainly an indicator that they are doing something wrong. It is rather worrying to note that in 2012, the average time between breach and discovery was 6 months, which had improved to just over one month by 2016, yet by 2017, it had returned to an average of almost 6 months again.

With an average time between breach and discovery of nearly 6 months, it is clear that the intruder will have more than enough time to amply cover their tracks by the time internal discovery would be possible. An important part of compliance is the ability to report to the regulator precisely which records were accessed, copied, modified or deleted. With forensic and audit trail data well and truly compromised or completely deleted, this cannot be achieved, meaning compliance is not possible. This, in turn, will mean the possibility of huge fines from the regulator. This will be particularly true where encryption is not used, meaning compliance breaches in regards to failure to be able to report properly to the regulator, failure to be able to comply with the Right to Access, the Right to Erasure, failure to know which data subjects to report the breach to, which could extend to millions of data subjects.

VI. Sensible Suggestions to Mitigate the Potential Impact of the GDPR

In Section IV, we have outlined the minimum requirements for compliance. In order to achieve this, there are certain tasks that must be performed. These are:

- 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.

VII. Proposed Pilot Study

We propose to carry out a pilot study using a private network, which will include a real physical miniature cloud warehouse, as well as real miniature conventional distributed systems. The components will comprise the following:

- An HP Microserver running a Intel Xeon E3-1275 V2 @ 3.50GHz processor, 16 GB of ECC fast server RAM, and a 525GB SSD which will run an Ubuntu server operating system, with a full Eucalyptus cloud computing environment;
- A number of Raspberry Pi2 devices with fast SanDisk Extreme Pro SDHC 32GB UHS-II cards set up to represent distributed systems servers running typical LAMP servers;
- A number of Raspberry Pi2 devices with fast SanDisk Extreme Pro SDHC 32GB UHS-II cards set up to represent attack desktops configured with Kali Linux as peneetration testing/attack desktops;
- A private Router;
- An HP 24 port network switch;
- all with hardwired LAN connections.

Additional Pi2 servers will be added to provide external storage. These will be configured with linux operating systems and an immutable database to simulate the secure collection of both forensic data and audit trail data.

This provides us with a complete miniature environment to carry out a real world simulation of various software configurations. The cloud environment will include both conventional cloud instances, and a test using miniature unikernel instances [44]–[46], which we will also be testing.

We have identified a number of goals that we seek to achieve:

- We want students to understand how to configure a system to ensure a high level of resistance to attack;
- We want students to understand how attacks against their systems will be carried out, and to properly

understand how any vulnerabilities contained in their systems can be exploited;

- We want professional penetration testers to give us their professional opinion on how well set up the systems are;
- We want to understand how our proposed cloud forensic solution can mitigate the challenges of complying with the GDPR.

VIII. What will our pilot study aim to achieve?

Our main goals are to provide an education to students, but a subsidiary goal will be to provide an element of proof that certain theories will work. Gaining access to university networks is a notoriously difficult process, and tends to be impossible in the event of any kind of ethical hacking or penetration testing being involved. Thus, by providing a fully closed IT environment which would replicate a real world IT environment, including cloud services as well as conventional distributed network systems, this would represent a worthwhile means of carrying out serious real world tests.

We will invite Masters students as part of their cyber security course to both defend and attack the systems to understand how to make them more resistant to attack. The first phase will involve performing a full setup of a server system hosting a typical web service with database back end. Some will be hosted on Raspberry Pi computers to simulate enterprise class distributed network, and some will be hosted on a cloud environment. The students will utilise a typical setup 'how-to', freely available to download from the internet. Once these systems are up and running, the next phase will involve another group of students with appropriate training attacking the web servers using Raspberry Pi desktops running Kali linux and a series of attack tools, to demonstrate how easy it is to penetrate these systems. All forensic and audit trail data will be collected and analysed, to demonstrate to the students how to spot signs of different types of penetration attacks.

The next phase will involve the original student group reworking the installation process, having identified all the areas of weakness in order to allow them to configure their servers far more securely. The attackers will again attack, and the hope is that the defending students will have learned enough to make the attackers job far more difficult to carry out. Again, all forensic and audit trail data will be collected and subsequently analysed to demonstrate how simple, yet effective changes can improve security by a vast margin.

In the final phase of the pilot study, all the student groups will then attempt to defend their systems against a number of professional penetration testers who will be attempting to attack their systems. We hope the students will take from this case study a greater understanding of the problems facing companies, and in particular, a better grasp in how some simple changes can have such a positive impact on improving cyber-security for their systems.

IX. Limitations and discussion

Our proposed approach is intended to provide a "real world" feel to students, in order to give them an experience of what it is like to try to defend a system in the real world. Equally, our approach is also designed to give them a clear idea of what attackers can do, and what the consequences of being able to retain a foothold in a system will be for the business. This should help to inform them of exactly what they will need to do to ensure compliance with the GDPR and other legislation and regulation.

Using simulation software will not provide the "real world" feel that we will achieve with our proposal. We believe our approach will provide a much better understanding of the problems all students will face in the outside world once they qualify. By this means, we hope to minimise the limitations of our approach, resulting in a better experience for students. Equally, we hope to gain confirmation that our proposals are workable as a means of helping to achieve compliance with the GDPR, especially for cloud environments.

Returning to our thoughts from the introduction, we open up our discussion to the reader regarding the Regulator for the EU GDPR. Will they go on to evolve into Carcharodon Carcharias Moderator Europa Universalis, perhaps enabling the EU to bridge the funding gap resulting from Brexit. Will they generate bigger cash flows from ever higher fines generated at an ever more voracious rate, resulting in mass business closures? Or will they really try to encourage all PII processors throughout the globe to up their game to the point where all systems become far stronger?

Do we want to see the worlds' oceans run red with the voracious predations of Carcharodon Carcharias Moderator Europa Universalis, or do we all want to see a massive improvement in PII for all individuals of the globe?

X. Conclusion

The GDPR will present a serious wake up call to many companies who have currently lost focus on preparing properly for this regulation. In this paper, we have warned of the dangers of Carcharodon Carcharias Moderator Europa Universalis developing this regulation into a dystopian future, possibly leading to the destruction of enterprise as we know it.

We have identified the key requirements to which all organisations falling under the jurisdiction of the regulation must comply. We have touched on the currently unresolved "Cloud Forensic Problem" as presenting the largest obstacle to achieving compliance for cloud use, and how continued undetected presence of intruders does the same for conventional distributed systems.

We have proposed a simple means as to how this challenging problem might be approached to ensure all IT system cloud users can be fully compliant with this new regulation, through little more than being sensibly organised. This will obviously involve additional cost 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.

We believe it is likely that our approach will ensure faster discovery of the occurrence of a breach. This will minimise the potential impact on business continuity, and we seek to prove this through the results of our pilot study.

We would certainly prefer to see this regulation used as a force for good to encourage all enterprises to up their game to ensure far higher standards of security and privacy for everyone on the planet. In this modern day and age, we should certainly be able to expect this as a basic human right.

REFERENCES

[1] B. Guttman and E. A. Roback, "NIST Special Publication 800-12. An Introduction to Computer Security: The NIST Handbook," NIST, Tech. Rep. 800, 2011. [Online]. Available: csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[2] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," Proc. - 2011 IEEE World Congr. Serv. Serv. 2011, 2011, pp. 584–588.

[3] 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.

[4] 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.

[5] 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.

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

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

[8] BLP, "UK government reveals data protection plans," 2017. [Online]. Available: http://www.blplaw.com/expert-legal-insights/articles/gdpr-and-brexit-uk-government-unveils-data-protection-plans

[9] Verizon, "2012 Data Breach Investigations Report," Verizon, Tech. Rep., 2012.

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

[11] 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

[12] R. H. Weber, "Internet of things–new security and privacy challenges," Computer law & security review, vol. 26, no. 1, 2010, pp. 23–30.

[13] C. Kuner, "The european commission's proposed data protection regulation: A copernican revolution in european data protection law," 2012.

[14] L. Costa and Y. Poullet, "Privacy and the regulation of 2012," Computer Law & Security Review, vol. 28, no. 3, 2012, pp. 254–262.

[15] I. Rubinstein, "Big data: the end of privacy or a new beginning?" 2012.

[16] A. Mantelero, "The eu proposal for a general data protection regulation and the roots of the right to be forgotten," Computer Law & Security Review, vol. 29, no. 3, 2013, pp. 229–235.

[17] M. L. Ambrose and J. Ausloos, "The right to be forgotten across the pond," Journal of Information Policy, vol. 3, 2013, pp. 1–23.

[18] B.-J. Koops, "The trouble with european data protection law," International Data Privacy Law, vol. 4, no. 4, 2014, pp. 250–261.

[19] C. Bartolini, G. Gheorghe, A. Giurgiu, M. Sabetzadeh, and N. Sannier, "Assessing it security standards against the upcoming gdpr for cloud systems," 2015.

[20] E. Luger, L. Urquhart, T. Rodden, and M. Golembewski, "Playing the legal card: Using ideation cards to raise data protection issues within the design process," in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 2015, pp. 457–466.

[21] B. A. Safari, "Intangible privacy rights: How europe's gdpr will set a new global standard for personal data protection," Seton Hall L. Rev., vol. 47, 2016, p. 809.

[22] G. Buttarelli, "The eu gdpr as a clarion call for a new global digital gold standard," 2016.

[23] G. Maldoff, "The risk-based approach in the gdpr: interpretation and implications," IAPP https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff. pdf. Accessed, vol. 12, 2017.

[24] J. Zerlang, "Gdpr: a milestone in convergence for cyber-security and compliance," Network Security, vol. 2017, no. 6, 2017, pp. 8 – 11. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485817300600

[25] B. Duncan and M. Whittington, "Can Forensic Audit Help Address the Cloud Forensic Problem in Light of the Requirements of the Forthcoming European Union General Data Protection Regulation?" in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 84–89.

[26] B. Duncan, "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?" in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 1–6.

[27] 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

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

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

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

[31] 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.

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

[33] 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.

[34] 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.

[35] B. Duncan and M. Whittington, "Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging," Int. J. Adv. Secur., vol. 10, no. 3&4, 2017, pp. 155–166.

[36] BIS, "2013 Information Security Breaches Survey," London, Tech. Rep., 2013. [Online]. Available: http://www.google.co.uk/url?sa=t{\&}rct=j{\&}q=2013informationsecuritybreachessurvey{\&}source=web{\&}cd=2{\&}cad=rja{\&}sqi=2{\&}ved=0CDMQFjAB{\&}url=https://www.gov.uk/government/uploads/system/uploads/attachment{_}data/file/191670/bis-13-p184-2013-information-security-breac

[37] Cisco, "2013 Cisco Annual Security Report," Tech. Rep., 2013. [Online]. Available: http://grs.cisco.com/grsx/cust/grsCustomerSurvey.html?SurveyCode=4153{\&}ad{_}id=US-BN-SEC-M-CISCOASECURITYRPT-ENT{\&}KeyCode=000112137

[38] Kaspersky, "Global Corporate IT Security Risks: 2013 The main findings," Tech. Rep., 2013.

[39] Verizon, "2013 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others," Tech. Rep., 2013.

[40] Great Britain. Department for Business Innovation and Skills, "2014 Information Security Breaches Survey: Technical Report," Tech. Rep., 2014. [Online]. Available: https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

[41] Verizon, "2015 Verizon Data Breach Report," Tech. Rep., 2015.

[42] Trustwave, "2016 Trustwave Global Security Report," Chicago, Tech. Rep., 2016.

[43] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016.

[44] B. Duncan, A. Happe, and A. Bratterud, "Cloud Cyber Security: Finding an Effective Approach with Unikernels," in Adv. Secur. Comput. Commun., J. Sen, Ed. InTech, 2017, p. Chapter 2.

[45] A. Bratterud, A. Happe, and B. Duncan, "Enhancing Cloud Security and Privacy: The Unikernel Solution," in Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization, 2017, pp. 1–8.

[46] A. Happe, B. Duncan, and Alfred Sewitsky Bratterud, "Unikernels for Cloud Architectures: How Single Responsibility can Reduce Complexity, Thus Improving Enterprise Cloud Security," in COMPLEXIS 2017 - Proc. 2nd Int. Conf. Complexity, Futur. Inf. Syst. Risk, Porto, Portugal, 2017, pp. 1–12.