Risk Management for Cloud Compliance with the EU General Data Protection Regulation

Bob Duncan*,Yuan Zhao†
Business School
University of Aberdeen, UK
Emails: *robert.duncan@abdn.ac.uk,†y.zhao@abdn.ac.uk

***Abstract*—Many cloud users are oblivious to the potential regulatory risks facing them should they be unable to comply with the EU General Data Protection Regulation (GDPR). As a result of one of the last minute changes to the GDPR last year, whereby instead of requiring reporting of a breach 'within 72 hours of the occurrence of that breach', it was changed to 'within 72 hours of discovery of a breach'. Until this subtle shift in the regulation took place, a great many companies were very focussed on cutting the time between breach and discovery. Now, a great many companies, both large and small, have breathed a huge sigh of relief, and stopped working on cutting down this time. Another change to the regulation extended the jurisdiction of the regulation from data processors located anywhere in the whole of the EU, to any data processor processing the data of any EU resident, anywhere in the world. Of course, this is only an issue if a breach takes place, but as this is no longer a case of if, but when, then companies would do well to be prepared for this inevitable certainty. For those companies who use cloud, there are additional considerations which must be taken into account, due to the Cloud Forensic Problem. This paper considers how companies should address many of the unexpected risks associated with the use of cloud in their organisations, and considers how they should go about monitoring their systems in order to get a much faster idea of who is getting into their systems, and understanding the full extent of the risks involved. Failure to comply brings serious consequences with it. Fines for a single breach can rise to the higher of €20 million or 4% of global turnover.**

Keywords–Risk management; Cloud forensic problem; GDPR compliance.

I. Introduction

All computing systems are under constant attack. For those companies using traditional networked computer systems, this presents a serious challenge to maintain a high level of security and privacy [1]. For those companies who use cloud systems, the challenge increases exponentially. This arises due to the increase in complexity in software, the multiplicity of layers and the number and range of actors involved in today's advanced cloud ecosystems.

There is still one serious, yet unresolved, remaining challenge — the cloud forensic problem. This challenge arises where an attacker breaches a cloud system, thus becoming an intruder. Once the intruder has a foothold in the system, usually without the company having the slightest idea of their presence, there is nothing then to prevent that intruder from attempting to escalate privileges to allow them remove all trace of their attack by deleting or modifying the forensic trail which records all their actions and routes into the system. Naturally, they are perfectly happy to remain hidden in the victim's system, continuing to steal ever more information, the longer they can continue to remain hidden.

Where a company both uses cloud, and is liable to fall under the jurisdiction of the forthcoming EU General Data Protection Regulation (GDPR) [2], this presents a decidedly difficult compliance challenge. Cloud users will be unable to meet compliance requirements by default, unless special measures are taken to address the risks involved. With the punitive level of possible fines for non-compliance (up to the greater of €20million or 4% of last year's global turnover), a compliance failure is likely to lead to a considerable financial impact on these companies.

Moving back to a distributed network solution is unlikely to be a viable option due to the long lead time required, the enormous costs involved, and the level of expertise needed to securely set up such systems. This will leave such cloud users very exposed to the risks involved. Thus it is vital that a viable solution be found in the meantime, and as soon as possible. In order to manage risk properly, we must first understand the nature of that risk, the probability of its occurrence and likely impact on the company.

We first start by addressing the cloud forensic problem to understand why it is such a GDPR compliance challenge for cloud users in Section II. Next, we examine the nature of cloud operational risks and consider what the likelihood of occurrence, and the resulting impact is likely to be of these events in Section III.

In Section IV, we consider the implications of managing risk, in particular understanding risk properly, assessing the probability of the risk occurring and developing strategies to mitigate the risk, while in Section V, we look at how we might effectively monitor our cloud systems to identify the presence of intruders in as short a time as may be possible. In Section VI, we consider whether such an approach might be sufficiently robust to provide assurance of effective compliance. In Section VII, we discuss our findings and consider future work, and in Section VIII, presents our conclusions.

II. The Cloud Forensic Problem and GDPR Compliance

We know that all computer systems are continuously under attack, and cloud systems are no exception. There is no such thing as a system that is immune to attack, and that is certainly the case for cloud systems. During the past decade, a great many research papers, such as [3]–[10], there have been many suggestions which have improved the level of security and privacy offered in cloud systems. In spite of such good quality

efforts, no solutions have yet been found to resolve the cloud forensic problem.

Once an attacker compromises a cloud system and gains even a small foothold, thus becoming an intruder, their next task is to escalate privileges until they are able to access and delete, or modify, the forensic logs in order to hide all trace of their insertion into the system. This permits them to retain a long term foothold within the system, providing them with a means to help themselves to whatever data they wish. They will usually seek to achieve this as quickly as they possibly can and usually succeed in a very short time frame [11]. They are often aided by the lack of scrutiny of server logs evident in many corporate systems.

Many companies neither retain records of which database records have been accessed, nor by whom, meaning that once breached, the company no longer has the ability to be able to report which records have been accessed, copied, modified, deleted or ex-filtrated from the system. This results in non-compliance with the GDPR, meaning exposure to potentially punitive levels of fines. To achieve compliance with the GDPR, companies must be able to report a breach within 72 hours of discovery. The global average time for all companies between breach and discovery in 2012 was an average of 6 months [12] [13]. This had improved to some 4 weeks by 2016 [14] — still far short of what is needed to understand what has been going on with the intruders while they were undiscovered.

However, as we noted in the introduction, the original plan for the GDPR was to insist that breach reporting take place within 72 hours of breach occurrence. The watering down of this part of the regulation to within 72 hours of discovery is somewhat counterproductive to compliance requirements of the GDPR. Companies no longer have the incentive to try to reduce the time between breach and discovery as they believe that as long as they comply with the ability to report the breach with 72 hours all will be well from a compliance perspective. This rather misses the point that the longer an intruder remains in a system undetected, the more damage or harm they can cause. Bearing in mind that encryption is not a requirement of the GDPR, then should a company choose not to encrypt, the damage caused by mass leakage persisting undetected for long periods of time will very much mean there will be little leeway to claim mitigation when it comes to the eventual fine by the regulator.

Where cloud is used, and in particular, where it incorporates any Internet of Things (IoT) use, this raises a question as to just how feasible compliance might really be. Compliance within such a tight time schedule might be all but impossible. If a company using cloud is breached, and especially if it has made no special arrangements to ensure the safety of forensic and audit trail data, the 72 hour deadline is moot. This is because the company will have no means of knowing that it has been breached, meaning there will be nothing to report. Of course, ignorance of the fact that a breach has occurred will not be a mitigatory factor. In any event, once discovery eventually does occur, usually through third party sources, there will be no prospect of ever finding out precisely which records have been compromised. Once the forensic and audit trails are gone — they are gone forever.

Where IoT is in use, this can introduce new troubles into the equation. The vast majority of IoT devices are usually cheaply made, with minimal resources, and often with insufficient or no security. The problem is not really the loss of the IoT device data, rather the fact that a skilled intruder can easily leverage these compromised devices to gain access to other more sensitive systems. Consider how the Mirai virus started as a simple attack on individual IoT devices, progressed to seeking out and leveraging other higher powered devices at scale to perpetrate massive Distributed Denial of Service (DDoS) attacks, to then identifying and penetrating sensitive PC networks after the virus was ported to Windows. Thus, it can be seen that any company utilising IoT devices will have particular compliance risks to face. We do not specifically address the IoT within this paper, but recognise that any company using IoT devices must take special measures to ensure GDPR compliance can be achieved.

Any company which is not prepared to take these special measures to safeguard their forensic and audit trail data will be far more likely to fail compliance in the inevitable event of a breach occurring. The likelihood of directly discovering a breach will be extremely low, let alone the possibility of being able to do so within 72 hours of the breach taking place. If, by chance, they were able to discover a breach within 72 hours, there is a very high probability that they would struggle to determine what to report in such a case. This is sure to be a factor in raising the level of the fine to which they would be liable.

It is obvious that the longer an intruder remains hidden inside a company system, the greater the damage they are likely to be able to do. Equally, if the company is unable to discover the breach within 72 hours of occurrence, it is highly unlikely that they will ever be in a position to discover the breach, let alone understand which records have been compromised. With no forensic or audit trails to follow, it will be completely impossible to determine what to report.

Not being able to discover that a breach has arisen will ensure that there will be no concern from the regulator. However, as inevitably happens with these matters, the leakage invariably becomes public knowledge, at which point, the regulator will become involved. If it can be shown that the company was negligent in its approach to safeguarding this personally identifiable information (PII) of data subjects, the penalties will surely rise significantly. There is no requirement specified in the GDPR to encrypt data. However, there is certainly a strong recommendation that this should take place, and within a reasonable time. The regulation suggests that encryption and decryption keys should not be stored on the cloud instance. Clearly, failure to consider these matters will lead to stiffer fines in the event of a breach.

Thus, in the next section, we shall take a look at how cloud users currently perceive cloud operational risk, and will consider whether this will be adequate for cloud compliance with the GDPR.

III. Cloud Operational Risks

Cloud operational risk refers to the actions that undermine the technical infrastructure and security assumptions relating to cloud based ecosystems. The Federal Financial Institutions Examination Council in 2012, in addressing the NIST definition of Cloud Computing [15], suggested addressing the following cloud operational risk areas:

- The use of market leading, experienced cloud service providers familiar with the financial industry and your Financial Institution's (FI) legal and regulatory requirements for safeguarding customer data and other sensitive data is a sensible idea;
- Backup, redundancy, and recovery are at the core of the decision to use an outsourcing vendor with highly redundant and resilient data centres designed for mission-critical applications;
- Internal controls and security processes can be negotiated by the FI to ensure customer information is appropriately segregated and protected by industry-standard compliance policies;
- Leading cloud providers continuously improve their hardware environments to ensure the latest versions of operating systems are installed and use agile software development to deploy feature/function releases on an accelerated basis;
- The use of tailored cloud deployment options to meet your specific needs including private clouds solely deployed on your behalf, or a hybrid cloud consisting of shared hardware but segregated data storage would be a prudent move;
- Outsourcing portions of your information technology infrastructure can free up internal IT resources to focus on strategic initiatives and new product development;
- Providers with financial services domain expertise reduce complexity and risk for FIs with their extensive knowledge of global standards, communications protocols and file formats;
- Cloud providers with global support centres can provide 24 x 7 support in multiple languages, ensuring your international clients and regional offices have access to the support resources required as problems arise.

This was the 'state of the art' of the day, and these issues have been well addressed in the intervening years. In 2011, NASA [16] were one of the early organisations to recommend using a risk based approach for identifying, recognising and dealing effectively with operational risk, particularly where complex IT systems are in use.

However, cloud has moved on significantly in the interim, and there are now some far more pressing matters that need to be dealt with, which we shall outline here. While these were very appropriate cloud operational risks to cover at the time, they do not cover the range of new risks faced, such as the cloud compliance risk associated with the use of cloud, while trying to comply with the new EU GDPR. We are aware of four main issues that must be dealt with as a matter of urgency within any organisation requiring to be GDPR compliant:

- *The Cloud Forensic Problem* This presents a huge potential problem where no special arrangements are in place, such as that a secure forensic and audit trail is maintained using a high security immutable database [17]–[20], and examination of all system access requests to determine the authority of all users to have authorised access to the system. Use of intrusion detection and authentication technology to automate the monitoring for attack attempts is also necessary [21];
- *Internet of Things (IoT)* IoT devices used for any purpose by cloud users present a considerable risk, mainly due to the often cheaply made devices with little or no security, often vulnerable to the Mirai virus, which can allow attackers to gain access to systems and to further compromise the main PC and server network due to the porting of the Mirai virus to be able to attack Windows computers [22], [23];
- *Proper monitoring of database access* – who, from where, when did they access the database, what did they see, modify, delete or exfiltrate from the system [24], [25]? This is a well known area, but it is clear that many companies expose themselves to exploitation by failing to take simple steps to mitigate the well known exploits currently in active use by attackers [20]. Some, like [26]–[28] propose the use of data provenance to ensure the integrity of data, with others proposing a new method of cloud forensic audit to assure the provenance of the data [29];
- *Encryption* Encryption is a good thing to consider [30], but there are caveats – first, the encryption and de-cryption keys must not be kept on the cloud instance. The encryption should be carried out offline in the cloud users' own systems before being transferred to cloud. Done properly, this can provide serious mitigation to the new EU GDPR fine levels, because if an intruder gets into the cloud system, all they get is encrypted data, which can take a great many years of substantial compute resources to de-crypt. With strong levels of encryption, it becomes practically impossible to crack [31] (of course, all this could change with the development and evolution of quantum computing, but that is another matter entirely).

Failure to deal properly with the above four risks will lead to very serious compliance breaches which can trigger punitive levels of fine by the regulator. But these risks are also capable of generating further problems for such companies. These risks can generate further risks in regard to business diminution; loss of share value; reputational damage risk; an emerging era of potentially serious regulatory fines, the serious expense of forensic investigations (massively expensive) after a breach, and the impact on business continuity.

In the next section, we move on to discuss how to identify, assess and manage these risks, particularly in regard to being able to deliver compliance with the special requirements of the GDPR.

IV. Managing Risk of Cloud Compliance for GDPR

The cloud compliance risks specific to achieving compliance with the EU GDPR cover the specific risks, the likelihood/probability of occurrence, the likely financial/corporate/personal impact of such a failure, and point to any mitigating strategies that might be used to mitigate the risks. It is of great importance to quantify these risk for financial risk management. Under financial management, four types of risk - credit, liquidity, market, and operational

- can affect the potential outcome/performance of financial investment for companies.

Companies have adopted various approaches to handle the oversight of cloud risks. Some share the primary responsibility among technology and risk committees, some particularly establish a special committee on cloud security. However, the cloud compliance for GDPR does not raise the same amount of attention in practice. The authors propose a few steps towards a more secure cloud environment in cloud compliance. The first step towards this goal is to establish a culture of cyber awareness at the organisational level. This is especially important when recent data suggests that company employee negligence or malicious acts contribute to nearly two thirds of cloud security breaches. The company also needs to elevate their access to cloud security expertise, by bringing in cyber security experts onto the board and the relevant committees. The third step is to ensue accountability and prioritization of cloud security, and also to develop a robust response to attack and provide effective recovery approaches.

A. The Main Risk Types

Turning to the four main risk types in financial systems, the first is credit risk. This is more frequently an issue in financial institutions where banks, for example, lend money to companies and individuals. Credit risk is the risk that the borrower will default on their payment. But this type of risk is not restricted to financial institutions alone. Virtually all companies provide lending to their customers in the form of trade accounts which offer credit terms. It is worth mentioning that in the case of business to business (B2B) lending, this may not expose the companies to a requirement to be compliant with GDPR, unless one company is providing a fulfilment service to the other which would involve the holding of PII.

A great many companies use cloud based accounting systems these days, and this can add an additional element of risk to the equation. In addition, where the customer is an EU resident, this serves to expose the company to require GDPR compliance. In addition, many companies will provide loans to other companies when they have a huge cash surplus, since they can obtain far greater rates of return than can currently be achieved from banks.

The second type of risk is liquidity risk. Liquidity risk is the risk that a company or bank may be unable to meet short term financial demands, otherwise known as 'running out of money.' This can arise due to the difficulty of converting some security or hard asset into cash, from poor management of debtors, or over-extending through poor cash management. There can be many other factors which can cause this risk, but the effects can be catastrophic.

The third type of risk is market risk. This is more frequently seen in financial institutions, where banks, for example, experience losses due to failings in the overall performance of the financial markets in which they are involved. Companies may also experience losses due to the way they make both short term and longer term investments of surplus business funds.

The forth type of risk is operational risk. This generally addresses all remaining risks, with the first three being the major risks that businesses and in particular financial institutions are exposed to. However, it is clear that the risks in this area are growing significantly. We have already discussed this, including identifying cloud operational risk in Section III, which we shall call the fifth risk.

However, as we can see from the title of this section, a new and potentially catastrophic risk, which we shall call the sixth risk, is compliance risk, in particular GDPR compliance risk. This new risk is likely to eclipse all previous compliance and indeed operational risks to a massive extent, and to that end, we must recognise this specifically and deal with it accordingly.

Other risks. We should also bear in mind that as soon as a new risk is identified and it is clear that the potential impact can be substantial, then it should also be separately identified and dealt with as a major part of the risk management process for the company.

B. The Likelihood or Probability of Occurrence

From security breach reports, we can see that the average number of breaches sustained by large corporates is running at 2 per week. Large corporates have the financial muscle to ensure high levels of security can be achieved. Smaller companies should bear in mind that without such financial muscle, and expertise available to them, they will be far more susceptible to attack, and thus will require to be far more vigilant as a result. The average number of attacks on small companies is estimated to be around ?? per week. Smaller companies are invariably much less well protected than large corporates, leading to many more successful attacks. Companies are generally very reticent to disclose attacks, although that will necessarily change with GDPR where disclosure to the regulator is mandatory.

Since every successful attack could lead to the requirement to report a breach to the regulator, and exposure to a potential fine, it is clear that this could lead to massive exposure to fines.

It is no longer a question of 'if', rather it is a matter of 'when' the breaches will occur, and of how far the intruder will reach into the company systems before they can be identified, dealt with and removed from the system. As we see from Section II and Section III, the Cloud Forensic Problem exposes cloud users to far more danger. The longer the intruder remains hidden within the system, the greater the danger. With the possibility of multiple attacks leading to multiple fines, this scales the potential severity of the attacks significantly, especially where both forensic and audit trail data is compromised.

C. The Likely Financial, Corporate or Personal Impact of Such a Failure

The likely financial impact from such failures will come from several sources. Money or assets may be stolen from the company. Fines may be levied for non-compliance. There may be reputational damage to the company, not least evidenced by a significant drop in the share price. This may also impact on future sales as customers may be put off by the insecurities inherent in any dealings with the company.

From the corporate perspective, the reputational damage may persist for long periods of time. There may also be an impact on business continuity management. The internal costs of dealing with breaches can escalate very quickly to frightening levels.

From a personal perspective, individuals affected by breaches can find they can have a potentially catastrophic impact on their lives. Their personal details can be widely

marketed on the dark web to countless numbers of criminals who will be only too happy to exploit such information to suit their own ends.

Under the GDPR regulation, the use of encryption is not mandatory. However, where encryption is properly implemented, this can go a long way to reducing the potential financial, corporate and personal impact. Given that many large companies are dealing with millions of customers, it is clear that failure to implement encryption would be foolhardy.

D. Potential Mitigating Strategies

We include here a list of suggested sensible steps which companies might take to mitigate the potential impact of the risks they face.

In [32], with Whittington, we demonstrated the importance of being able to properly identify risk, in order to be able to carry out proper mitigation strategies. If a company is unable to identify the risk, there is likely to be little prospect of any effective mitigatory steps being taken. Returning to our identified areas of risk, we consider our potential mitigating strategies.

Most financial institutions have long been obliged to identify risk, develop mitigating strategies and to report on these efforts in great detail in their annual report. Indeed, after the financial crisis of 2008, risk reporting requirements have increased significantly, and in some cases have increased to several hundred pages of detail given in the annual report. Thus, we consider the main risk areas in the context of the majority of companies. Of course, many of the mitigating strategies we discuss will apply equally to financial institutions who use cloud systems, even where the cloud systems used are private cloud systems.

Credit risk:

- Thoroughly check a new customer's credit rating
- Use the first sale to start building the customer relationship
- Establish credit limits
- Make sure the terms of credit of sales agreements are clear
- Use credit and/or political risk insurance
- Possibly use factoring, but it must be on a non-recourse basis, where the factor accepts the customer default risk
- Develop a standard process for handling default customer accounts

Liquidity risk — companies can learn from the suggestions of the Basel committee for banks:

- Identify liquidity risks early
- Monitor and control liquidity regularly
- Conduct scheduled stress tests
- Create a contingency plan

Market risk — again companies might learn from the approach taken by banks to hedge against market risk:

- Use of modern portfolio theory to spread risk
- The use of options could also be considered as a hedge
- Index options are another possibility
- Use of the volatility index (VIX) indicator, perhaps in conjunction with options
- However, options do degrade as they near expiry, and it may also not be economic to hedge every possibility

Operational risk:

- Use of market leading CSPs
- Highly robust backup, redundancy and recovery are core requirements
- Internal controls must extend into the cloud space
- Ensure the CSP uses the most up to date hardware and software
- The use of tailored solutions, including private cloud, hybrid or shared hardware with segregated data storage
- Proper outsourcing of IT frees up internal resources to concentrate on core business needs
- CSPs with domain specific expertise can reduce complexity
- CSPs with global support centres can provide 24x7 support for global customers

Cloud operational risk:

- Ensure the cloud forensic problem is adequately addressed
- Where IoT is used, ensure extra measures are put in place to defend against all currently known weaknesses, and ensure Intrusion detection is robust and fully active
- Ensure proper monitoring of database access is carried out, with automated detection of anomalous behaviour regularly reported
- Use a strong level of encryption is used, and set up so that encryption and decryption keys are not stored on any cloud instance

GDPR compliance risk:

- Prevent failure to realise a breach has occurred by ensuring the cloud forensic problem is adequately addressed
- Prevent failure to be able to report a breach properly, by ensuring full retention of protected forensic records and the audit trail
- Prevent failure to protect data subject's PII, by ensuring proper encryption is used for all data in transit and at rest
- Pseudonymisation and anonymisation are also valid forms protection that could be used
- Prevent failure to protect the company cloud system properly, by ensuring the encryption and decryption keys are not stored on the cloud instance

V. Implementing an Effective Means of Monitoring for Intruder Detection

In previous work [24], [33], Duncan and Whittington emphasised the importance of ensuring continuous monitoring takes place to ensure the integrity of cloud data over time, and to be able to identify intruders at the earliest possible time. Neovius and Duncan demonstrated a possible solution for detecting anomalous behaviour in cloud accounting systems [21], and Kratzke demonstrated a human biology inspired method of intruder detection and self healing of systems [34].

The best approach is always to use something that is simple. Complex systems tend to be very difficult to configure properly, and the output is often left lying unused, because analysis proves so difficult to achieve, and is frequently beyond human comprehension. If the system is simple and straightforward to use, then the output will be simple to analyse programmatically, meaning management by exception becomes a distinct possibility. Systems that are easy to use, generally are used frequently.

It is obvious from the continuing challenge for companies to reduce the time between breach and discovery [23], that many companies still fail to examine their forensic and audit trails sufficiently meticulously to identify the presence of possible intruders. Once these intruders have escalated privileges to allow them to delete the forensic trail, then there is very little chance of recovering easily from that scenario. Without the data being encrypted properly, there is then a real possibility the the GDPR regulator will exert their power to raise fines at a punitive level.

In [18], [35], Duncan and Whittington proposed a simple yet effective solution which demonstrated how to ensure that a robust forensic and audit trail might be secured at minimal expense.

VI. Would such an Approach be Sufficiently Robust to Provide Assurance of Effective Compliance?

Under the GDPR [36], cloud users who fall under the jurisdiction of the regulator must be able to demonstrate compliance with the regulation. This means they should be able to show they have taken proper precautionary steps to ensure they have been able to maintain the integrity, security and privacy of data belonging to data subjects covered by the regulation. By putting in place the suggestions we have made, the company will be able to demonstrate a high level of effective monitoring, the use of good security techniques, and the proper use of encryption.

In the event of a security breach, they will readily have access to the means of identifying the culprits, the means by which the breach was perpetrated, and a detailed account of which records may have been affected. This will clearly demonstrate a serious approach to the regulator. However, where encryption has been properly used, it is unlikely that the regulator will be overly exercised about the effects of the data breach, since the data stolen will be effectively useless to the intruder. The regulator will not even require the company to contact the affected data subjects, since there will be no practical danger to them individually.

We can demonstrate through implementing these suggestions that we can achieve a robust and high level of compliance to the regulator, which will ensure we can minimise the impact of these risks on the company. On the other hand, it is very clear that by not having these measures in place, compliance with the GDPR is likely to be an impossibility, leading to the prospect of substantial fines in the future, when the breaches inevitably start to occur.

VII. Discussion and Future Work

As we can see from this paper, GDPR compliance will be far from easy to achieve, and for cloud this will be especially problematic and challenging. For a great many organisations, the GDPR brings a great many risks to bear when considering compliance with the GDPR. They come from a great range of sources, and the biggest risk of all is likely to come in the form of failure to recognise just how important it is to identify and mitigate these risks properly.

A great many companies will not be able to recognise these risks, particularly those who do not have the financial clout to provide the right level of expertise, meaning that they will be even more exposed than those who do have the means to recognise and address these risks. There is no doubt that these risks are significant, and potentially devastating for the company should they fail to achieve compliance with the GDPR.

We hope that this paper might start to provide them with some idea of what is required to achieve compliance, and what the implications might be for compliance failure. The steps outlined here are straightforward to implement. The most important being that in order to deal with a risk, the company must first recognise the risk, and in order to do that, must have an understanding of what these risks might be and how they might go about mitigating the potential impact of these risks.

The GDPR comes into effect on 25th May 2018, and for a great many companies, they will be sitting ducks as far as the regulator is concerned. Yet, by taking some basic, elementary steps, they could go a long way towards mitigating this potentially devastating impact on their business. It is not merely enough to say that they will deal with reporting after they discover the breach. By that time, it may already be too late to find the necessary details with which to compile their report.

There will be a need to carry out some serious testing in order to find a satisfactory equilibrium between security, privacy, performance, reliability, accessibility and the accountability we require for GDPR compliance. To that end, we plan to conduct a pilot case study on how the technical aspects might be implemented in order to meet all the required goals to ensure compliance can be achieved. This will run around a miniature cloud system, offering both cloud-based and non-cloud based systems to assess what the optimum configuration might be. This will allow us to ascertain how well the cloud-based solution can match the capability of the non-cloud based system, after taking into account the impact of the cloud forensic problem.

VIII. Conclusion

For any company using cloud, it is clear that it will prove impossible to achieve compliance with the GDPR in the event of a security breach where they have not at least dealt properly with the as yet unresolved, cloud forensic problem. Claiming

ignorance of this problem following a cyber breach will not be sufficient grounds for mitigation of the fine by the regulator after the fact. It will certainly be too late by then. Thus, cloud users who must be compliant with the GDPR will have to take steps now to be thoroughly prepared ahead of time.

We have looked at traditional cloud operational risks and the new risks relating to coping with these unresolved problems and discussed how to go about resolving them, using wherever possible simple, yet effective, approaches to ensure a robust solution that will be both easy to implement and easy to maintain. By this means, we can eliminate a large amount of the risk. We accept that all risk will not be entirely removed, but there can be a significant reduction in risk levels involved. More importantly, it will be possible to demonstrate a high level of compliance with the GDPR.

Implementing these proposals should ensure that a healthy level of compliance can be achieved, without the need for expensive, complex solutions that could prove highly expensive to implement and maintain.

REFERENCES

[1] M. Westerlund and J. Enkvist, "Platform Privacy: The Missing Piece of Data Protection Legislation," J. Intell. Prop. Info. Tech. & Elec. Com. L., vol. 7, 2016, p. 2.

[2] EU, "EU General Data Protection Regulation," 2017. [Online]. Available: http://www.eugdpr.org/ Last accessed: 5 May 2018

[3] S. Pearson and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 5931 LNCS, no. December, 2009, pp. 131–144.

[4] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, no. December. IEEE, nov 2010, pp. 693–702.

[5] L. J. Sotto, B. C. Treacy, and M. L. Mclellan, "Privacy and Data Security Risks in Cloud Computing," World Communications Regulation Report, vol. 5, no. 2, 2010, p. 38.

[6] 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," Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011, 2011, pp. 584–588.

[7] D. Pym and M. Sadler, "Information Stewardship in Cloud Computing," International Journal of Service Science, Management, Engineering, and Technology, vol. 1, no. 1, 2010, pp. 50–67.

[8] J. Bacon, D. Eyers, T. F. J.-M. Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch, "Information Flow Control for Secure Cloud Computing," IEEE Transactions on Network and Service Management, vol. 11, no. 1, 2014, pp. 76–89.

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

[10] C. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," IEEE Transactions on Services Computing, vol. 9, no. 1, 2016, pp. 138–151.

[11] T. Micro, "Anatomy of a Cyber Breach," 2011. [Online]. Available: [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/110/anatomy-of-a-data-breach Last accessed: 5 May 2018

[12] PWC, "UK Information Security Breaches Survey - Technical Report 2012," London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com www.bis.gov.uk Last accessed: 5 May 2018

[13] Trustwave, "2012 Global Security Report," Tech. Rep., 2012. [Online]. Available: https://www.trustwave.com/Resources/Library/Documents/2012-Trustwave-Global-Security-Report/ Last accessed: 5 May 2018

[14] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016. [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf Last accessed: 5 May 2018

[15] P. Mell, T. Grance, and Others, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Tech. Rep., 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final Last accessed: 5 May 2018

[16] M. Stamatelatos and H. Dezfuli, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," NASA, Tech. Rep. December, 2002. [Online]. Available: http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf Last accessed: 5 May 2018

[17] B. Duncan and M. Whittington, "Cloud cyber-security: Empowering the audit trail," International Journal on Advances in Security, vol. 9, no. 3 & 4, 2016, pp. 169–183.

[18] B. Duncan and M. Whittington, "Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging," International Journal On Advances in Security, vol. 10, no. 3&4, 2017, pp. 155–166.

[19] B. Duncan, "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?" in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 1–6.

[20] B. Duncan, A. Happe, and A. Bratterud, "Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance," in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 71–76.

[21] M. Neovius and B. Duncan, "Anomaly Detection for Soft Security in Cloud based Auditing of Accounting Systems," in Closer 2017 - 7th International Conference on Cloud Computing and Services Science, Porto, Portugal, 2017, pp. 1–8.

[22] B. Duncan and M. Whittington, "Cyber Security for Cloud and the Internet of Things: How Can it be Achieved?" Cybersecurity: The Institution of Engineering and Technology, vol. Cybersecur, no. September, 2017, pp. 1–39.

[23] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017. [Online]. Available: https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/ LAst accessed: 5 May 2018

[24] B. Duncan, M. Whittington, M. G. Jaatun, and A. R. R. Zúñiga, "Could the Outsourcing of Incident Response Management Provide a Blueprint for Managing Other Cloud Security Requirements?" in Enterprise Security Springer Book 2016, V. Chang, M. Ramachandran, R. Walters, and G. Wills, Eds. Springer, 2016, pp. 1–22.

[25] B. Duncan, A. Bratterud, and A. Happe, "Enhancing Cloud Security and Privacy: Time for a New Approach?" in Intech 2016, Dublin, 2016, pp. 1–6.

[26] T. F. J. Pasquier, J. Singh, J. Bacon, and D. Eyers, "Information Flow Audit for PaaS Clouds," InCloud Engineering (IC2E), 2016 IEEE International Conference on 2016 Apr 4 (pp. 42-51). IEEE.

[27] N. Papanikolaou, T. Rübsamen, and C. Reich, "A Simulation Framework to Model Accountability Controls for Cloud Computing," CLOUD COMPUTING 2014, The Fifth International Conference on Cloud Computing, GRIDs, and Virtualization, no. c, 2014, pp. 12–19.

[28] T. F. J. M. Pasquier and J. E. Powles, "Expressing and Enforcing Location Requirements in the Cloud using Information Flow Control," Proceedings - 2015 IEEE International Conference on Cloud Engineering, IC2E 2015, 2015, pp. 410–415.

[29] 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 Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 84–89.

[30] V. Chang, M. Ramachandran, Y. Yao, Y. H. Kuo, and C. S. Li, "A resiliency framework for an enterprise cloud," International Journal of Information Management, vol. 36, no. 1, 2016, pp. 155–166.

[31] T. Pasquier, B. Shand, and J. Bacon, “Information Flow Control for a Medical Records Web Portal,” Cl.Cam.Ac.Uk, 2013, pp. 1–8.

[32] B. Duncan, Y. Zhao, and M. Whittington, “Corporate Governance, Risk Appetite and Cloud Security Risk: A Little Known Paradox. How Do We Square the Circle?” in Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Athens, 2017, pp. 1–6.

[33] B. Duncan and M. Whittington, “The importance of proper measurement for a cloud security assurance model,” in Proceedings - IEEE 7th International Conference on Cloud Computing Technology and Science, CloudCom 2015, Vancouver, 2015, pp. 517–522.

[34] N. Kratzke, “About an Immune System Understanding for Cloud-native Applications - Biology Inspired Thoughts to Immunize the Cloud Forensic Trail,” in Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, Barcelona, Spain, 2018, pp. 31–38.

[35] B. Duncan and M. Whittington, “Creating an Immutable Database for Secure Cloud Audit Trail and System Logging,” in Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization. Athens, Greece: IARIA, ISBN: 978-1-61208-529-6, 2017, pp. 54–59.

[36] EU, “EU General Data Protection Regulation,” 2017. [Online]. Available: http://www.eugdpr.org/ Last accessed: 5 May 2018