Cost-Effective Permanent Audit Trails for Securing SME Systems when Adopting Mobile Technologies

Bob Duncan
Department of Computing Science
University of Aberdeen
King's College, Aberdeen, UK
Email: robert.duncan@abdn.ac.uk and
Arcada University of Applied Sciences
Jan-Magnus Janssons plats 1, 00550 Helsinki, Finland
Email: robert.duncan@arcada.fi

Magnus Westerlund
Department of Business Management and Analytics
Arcada University of Applied Sciences
Jan-Magnus Janssons plats 1, 00550 Helsinki, Finland
Email: magnus.westerlund@arcada.fi

***Abstract*—Cyber security for SMEs is a challenging activity. Since large corporations started to improve their cyber security process and strategies, this has made life considerably more challenging for attackers. This has resulted in a change of approach by attackers to pursuing SMEs. They have found such companies to be far less focussed on achieving really tight systems that are difficult to penetrate, to the extent that they would rather attack SMEs than large corporations. This is an important problem to deal with, because while large corporations who get successfully breached find the result expensive and time consuming to rectify, they usually have adequate reserves and resources to survive. This is seldom the case for SMEs, and up to 50% of successful breaches on SMEs can result in their bankruptcy. However, since SMEs have neither the reserves, resources nor sufficient skill levels of employees to help them deal with this difficult challenge, they are left at a considerable disadvantage. We propose a simple, economic approach that can improve security, ensure retention of a full forensic trail, all within their financial means.**

***Index Terms*— SMEs, mobile devices, cloud security, audit trails**

I. Introduction

There is little doubt that keeping corporate systems secure presents a major challenge for businesses and in the UK, the Government Cyber Security Breaches Survey in 2020 [1] noted that almost half of all business suffered a breach during the previous year. While many large corporations have the necessary expertise and resources to deal with breaches, the same cannot be said for Small and Medium Sized Enterprises (SMEs). Why do we care about SMEs? Based on the World Trade Report, the International Federation of Accountants (IFAC) note that SMEs represent over 90% of the business population, 60-70% of employment and 55% of Gross Domestic Product (GDP) in all of the developed economies [2]. For SMEs, there are often serious constraints on resources, and limited expertise in this area among employees.

We have also seen a rapid evolution in business architecture, leading to new paradigms, such as cloud, distributed systems and so on. The evolving widespread shift to mobile communications and the ever increasing power of mobile phones, means that many employees will no longer operate just from a desk with a desktop computer, but instead might use a range of devices. Often any individual might have, in addition to the desktop, a laptop, a tablet, a mobile phone, or two, perhaps a smart watch to name but a few. These changes can offer improvements to the way business can operate more efficiently, but they also bring more risk. The traditional approach to security has been the "castle" approach to protect the centralised systems. Now add to this the effects of the pandemic and the move to working-from-home, often using completely insecure domestic network connections to add to the already precarious security approaches, and it is clear that a great many SMEs could be heading for disaster.

With limited expertise and resources and often limited understanding of the risks they face, this can put them at a serious competitive disadvantage. Perhaps far more worrying, will be the impact of their limited resources to spend on proper cyber security, leading to a continually increasing risk footprint. Another example might be that instead of using the largest Cloud Service Providers (CSPs) operated by 'big tech' companies such as Amazon Web Services, Microsoft Azure and Google Cloud, as well as traditional large corporations such as IBM and HP, many might be tempted to use smaller firms offering cheaper services, but who do not have the same security procedures in place as can be provided by the big CSPs.

Another important incentive concerns the ability to be compliant with ever more legislation and Regulation specifically targeting the proper control of Personally Identifiable Information (PII), such as we have seen with the introduction of the EU General Data Protection Regulation (GDPR). For a GDPR breach involving the PII of any EU resident, and UK residents, since it has been adopted by the UK since Brexit, fines can be levied at up to the greater of €20 million or 4% of annual turnover.

In Section II, we will consider the background on cyber security risks. In Section III, we will consider Cyber Security and SMEs and will introduce the framework for this interpretative study, where we will address Cyber Security Threats, SME behaviours, SME awareness and SME decision-making.

In Section IV, we will consider some proposed corporate solutions, looking at how these might be overly complex and costly for SMEs to adopt. In Section V, we will consider how we could adapt these for SMEs in a more cost-effective and simple way to make them attractive to SMEs to implement. Finally, in Section VI, we will discuss our conclusion.

II. Background on Cyber Security Risks

Proper risk management for SMEs has become an ever more urgent and serious problem to address, often due to the availability of minimal resources and limited understanding of why this could be such a vital asset to the company [3]. All companies face a continuously increasing range of risk. While traditional disaster type risks are reasonably easy to understand, when it comes to data, the majority of these risks are adversarial risks, which can be much more difficult to predict, and thus identify properly. The big problem for SMEs, is that they stand a much higher chance of going bankrupt after a large breach, due to their much lower level of available resources [4].

Almost 40 years ago, Hollman and Mohammad-Zadeh [5] recognised the importance of proper risk management for SMEs, and 8 years later Miller [6] developed a very straightforward framework suitable for SMEs to use for this purpose. While the risks faced since that time have changed significantly, that is no excuse not to bother doing a good job of risk management, as the ultimate risk if nothing is done could lead to bankruptcy.

Falkner and Hiebl [7] suggested that SMEs generally faced 6 main categories of risk:

- Interest rate risk;
- Raw material price rise;
- E-business and technology risks;
- Supply chain risks;
- Growth risks;
- Management and employee risks.

The authors suggest that it is clear the area that SMEs need to focus on will be E-business and technology risks, and in particular, cyber security risk management. The vast majority of such risks faced are adversarial in nature, making them a much bigger challenge to deal with properly. Research in this area has been a bit on the sparse side, but back in 2003, Tranfield et al., [8], put some useful base information together in their paper that provides a good understanding to start from. It is very clear that the more SMEs can start to understand the true nature of the risks they face, the better they will be able to prepare themselves to defend against them.

III. Cyber Security and SMEs

Recently, Alahmari and Duncan [9] wrote about the challenges faced by SMEs and wrote about 5 areas of importance that ought to be considered:

- Cyber Security Threats in SMEs;
- Cyber Security Behaviours in SMEs;
- Cybersecurity Practices in SMEs;
- Cybersecurity Awareness in SMEs;
- Cyber Security Decision-Making in SMEs.

Thus we will consider their observations in each of the following 5 sub-sections:

A. Cyber Security Threats in SMEs

One of the key takeaways from this area is that a major challenge is to be able to articulate properly the concept of what exactly cyber security is and how it can impact on their business. Some of the key risks arise from cyber attacks that seek to breach data systems in order to steal, modify or delete data, or to make it inaccessible to the users of the business [10]. To this day, these risks continue to present the same level of challenges, other than that the frequency of such attacks has intensified during the past 7 years [11]. It is noticeable that attacks against SMEs have also increased during the pandemic.

On the risk assessment front, Barlette et al., [12], suggest it can be challenging for SMEs to be able to quantify exactly what the impact of breaches can be. The authors also suggest that while many SMEs believe they are not vulnerable because of their size. That is precisely why they are being attacked, since they present a much easier target than large corporations, due to their limited resources and understanding of what they face.

B. Cyber Security Behaviours in SMEs

Barlette et al., [12] also suggest that employee behaviour can expose SMEs to greater threats due to such practices as ignoring information policies, organizational guidelines, and company rules can lead to exposing the SME to much greater risk. Training and education are vital tools that can be used to improve user awareness. Of course, in some cases, [13], this might still not be enough, as they found in a previous study that while training uptake was 85%, the actual behaviour was much lower at 54%.

There is little doubt that user commitment and behaviour are vital elements that can play a significant role in the success of the business's ability to achieve a high level of security [14]. Indeed, Gundu [13] avers that the real problem is not employees knowledge and understanding, rather it is their general negative cyber security behaviour as a whole that is the cause.

C. Cyber Security Practices in SMEs

It has long been a concern in the literature that the SME approach to cyber security has been the lack of seriousness. SMEs have often failed to respond to the warnings coming from the cyber security community about cyber threat [15], and observations have often been made of how authorised people participate, albeit unconsciously, in risky practices which could have an adverse impact on the cyber security success of the SME.

Osborn and Simpson [16], suggest that most cyber security experts believe that current security practices used by SMEs could be a barrier to efficiency due to the lack of their engagement with the research community. The authors believe that is such a pity, since large corporations are benefitting greatly from that relationship. While adopting outsourcing facilities such as the cloud could make a big contribution to the cyber security success of SMEs, their effectiveness would be seriously degraded by bad practices. As Bada et al., [17], suggest, failure to change those practices will perpetrate the continuing success of attackers leading to ever more attacks.

D. Cyber Security Awareness in SMEs

SME awareness of cyber security risks has traditionally been low, and Kaur and Mustafa, [14], suggest this has continually led to considerable risks to SME assets. Osborn and Simpson argue that the lack of knowledge of SME users significantly detracts from their awareness of cyber attacks, which leads to an adverse impact on achieving an adequate level of cyber security.

Osborn, [18], suggests that SMEs need additional information about possible vulnerabilities, rather more than they need the implementation of tools for evaluating self-assessed risks, meaning they should develop the content of their specific awareness programmes immediately. Gundu [13], suggests that creating the best possible awareness program could be far more productive for SMEs as a help to reduce the potential risks to an acceptable level.

The threat to cyber security has been recognised as the greatest threat to SMEs and that addressing this challenge by deploying protective measures alone is not enough. Kabanda et al., [15], suggest that increasing awareness is likely to have a far more positive impact.

E. Cyber Security Decision-Making in SMEs

In considering decision-making in information risk management, SMEs have adopted out-sourcing as part of their digital strategy. Successful out-sourcing has improved the web presence of SMEs and increased efficiency. However, outsourcing may have created a cyber security knowledge gap in SMEs. If cyber security is recognised, it is seen as a secondary issue to the presence. There is a lack of focus on security by design methodology in SMEs. Owners and managers generally play a major role [19] [12] [15], which demonstrates the importance that is understood at a managerial level. Such a pity that by the time it gets to implementation in SMEs that such poor results are achieved.

IV. Existing Corporate Solutions

In this section, we will take a look at a number of corporate solutions which have been developed to address a number of key areas to give a flavour of what large corporations can achieve with their vast reserves, resources and in-house expertise, in collaboration with the research community.

In 2016, Duncan and Whittington warned about forensic issues which they described as the Cloud Audit Problem [20], [21] and proposed a possible approach, although warning of some of the potential barriers faced. They followed this in 2017 with a suggestion on how to create such an immutable database and how to set it up to carry out such a task.

In 2018, Duncan and Zhao [22], considered the use of blockchain as an alternative to some of the conventional databases, which were limited in what they could do. At this time Neovius et al., [23] looked at the use of distributed ledger technology to provide much higher level security, and later adapted this approach to address IoT security weaknesses [24].

In 2019, Westerlund and Jaatun [25], addressed the challenge of dealing with the cloud forensic problem, while ensuring compliance can be achieved with the GDPR

In response to the serious weaknesses inherent in Internet of Things (IoT) devices, Wikström et al., [26] developed a high security approach using blockchain, but this time incorporating Ethereum smart contracts to extend the power of the work. This work would go on to be implemented to demonstrate the viability of the concept.

It would be important to recognise that these concepts were specifically targeted towards large corporations, meaning that they would have both sufficient resources available to develop and implement the full system and also would have sufficient in-house expertise to ensure proper configuration for the implementation would be carried out.

We must be clear that the required level of resource availability and in-house calibre of staff would likely be far in excess of anything that a great many SMEs would be able to provide. Thus we considered how we might come up with an effective, yet economical approach that could allow them to greatly improve their security capabilities.

V. Adapting Existing Corporate Solutions

The key requirement was therefore to keep it simple and find an approach that would be relatively straightforward to provide a much higher level of cyber security, without pushing them beyond their often constrained budgets. We also considered the fact that not all SMEs are equal. They might vary from a one man operation up to a large company size with many employees, much more resources than the smallest, and possibly more technically competent staff as well.

We decided to attempt to propose a basic level approach, then add incremental options depending on the resources and in-house expertise of the SME.

Even the smallest SME would likely operate with a considerable range of disparate devices, many of which would use different operating systems, different software and apps, which presents many SMEs with their first challenge. With insufficient resources and limited skills in the workforce, how could they do anything constructive from there?

Asking them to make changes to devices, or to update specialised software, would likely be a challenge too much for many. In many cases, there could also be a further issue, namely the Bring Your Own Device (BYOD) approach in many SMEs. Added to this would be the recent trend towards Working From Home (WFH) brought on by the Covid-19 pandemic.

A. The Basic Proposal

We felt the sensible thing would be to re-think how we might accomplish dealing with costly solutions for SMEs with very limited resources. Since all devices used offsite, and with the BYOD use in the office, the sensible approach would be to set up a Virtual Private Network (VPN), require all sign-ins to corporate systems to be addressed through the VPN and capture the forensic records in one place. In this way, no mater whether company devices, BYOD devices on users working on site could all login to the VPN, which would provide better security and privacy and the relevant data collected from the VPN without any company users noticing any change in what they had to do, other than a new login method. In this way, all direct logins to the company systems could be blocked to enforce login via the VPN.

Many large providers can deliver a cloud-based VPN service for a very reasonable monthly cost. They can also provide systems geared for growing businesses. It is possible to rent a company dedicated server to ensure increased availability and having connecting up/down speeds of 1Gbps. These company based solutions offer a dashboard to monitor and control what is going on with the company network. An SME without any other provisioned public endpoints than a VPN, would be able to effectively block off external system access. Certain providers can also offer VPN access based on multi-factor authentication (MFA) that further strengthen the authentication by utilizing a secondary key. Hence, if user id and password combination leak, a secondary physical key will still hinder unauthorized VPN access.

We would need to add an immutable database, and a new open source offering came to market just over a year ago, called immudb, which offers the fastest of database capabilities without it being possible to tamper with the data contained within the database. This addresses all of the traditional issues with slow or unusable systems. The combination of the use of the VPN in conjunction with the immutabe database, not only addresses improving the security of access systems, it also offers to ensure complete forensic trails are maintained, all without the need for SMEs to to spend huge sums the simply do not have.

The immutable database can be be kept remote from the VPN server and could even be based on a cloud system. As long as security is tight for this server, then it will provide exactly what any SME would wish to have. A full forensic trail of every device attempting to access company systems. In this way, the company will be assured that only staff accessing company systems would be able to be granted access. All external users of company systems would effectively be blocked off completely, leading to much tighter security for the SME.

This setup could include ALL devices, including mobile phones, but some companies might prefer to have a more structured approach. We therefore look at how we might meet this need.

B. Adding Mobile Devices to the proposal

In the business world, the most popular mobile phone systems use either Android operating systems, as developed by Google, or Apple systems for a more up-market approach. Google, for example, offer a mobile desktop package that provides a management dashboard, known as Android Enterprise. This can be developed in conjunction with Google. The mobile is connected through the VPN, using a business profile configuration, thus allowing the corporation to monitor for threats and hinder access.

VI. Conclusion and Future Work

SMEs must realise that they can no longer afford to ignore the need to pay serious attention to detail in matters of security. They must also start to realise that in order to remain compliant with the range of legislative and regulatory compliance, there is a strong need to address cyber security risks head on.

Legislators and regulators will not accept any excuses when it comes to cyber breaches, especially where personally identifiable information is involved. There are no excuses, and the legislators and regulators are right to bring those companies who fail to keep users' data properly secured to account.

These proposals we have offered provide a minimum step on the route to proper security. This needs to be done properly, and we do recognise that many SMEs simply do not have the resources to achieve a robust level of security. These proposals offer a potential route to achieving a much improved level of security for an extremely modest cost. With the bare minimum of expense, an SME could begin the process of bringing their systems to a much more robust level.

It is fair to say that these proposals are designed as a first robust step, and there will be considerable improvements that can be made in future. This proposal allows for the easy add-on of additional protections, thus building on what would already be there.

We plan to test this approach in the near future to demonstrate how well this basic approach can work for SMEs. Once we confirm the effectiveness of the approach, we would look to develop the extra advances that would allow additional new features to be added.

References

[1] HMG, "UK Cyber Security Breaches Report 2020," HMG, London, Tech. Rep., 2020. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020 [Last Access: 25th February 2022]

[2] IFAC, "The Foundation for Economies Worldwide is small business." [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity [Last Access: 25th February 2022]

[3] J. Brustbauer, "Enterprise risk management in SMEs: Towards a structural model," *International Small Business Journal*, vol. 34, no. 1, pp. 70–85, 2016.

[4] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision support systems*, vol. 86, pp. 13–23, 2016.

[5] K. W. Hollman and S. Mohammad-Zadeh, "Risk management in small business," *J. Small Bus. Manag.*, vol. 1, pp. 47–55, 1984.

[6] K. D. Miller, "A framework for integrated risk management in international business," *Journal of international business studies*, vol. 23, no. 2, pp. 311–331, 1992.

[7] E. M. Falkner and M. R. W. Hiebl, "Risk management in SMEs: a systematic review of available evidence," *The Journal of Risk Finance*, 2015.

[8] D. Tranfield, D. Denyer, and P. Smart, “Towards a methodology for developing evidence-informed management knowledge by means of systematic review,” *British journal of management*, vol. 14, no. 3, pp. 207–222, 2003.

[9] A. Alahmari and B. Duncan, “Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence,” in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE, 2020, pp. 1–5.

[10] K. Renaud and G. R. S. Weir, “Cybersecurity and the Unbearability of Uncertainty,” in *2016 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2016, pp. 137–143.

[11] A. A. Alahmari and R. A. Duncan, “Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs,” in *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2021, pp. 1–6.

[12] Y. Barlette, K. Gundolf, and A. Jaouen, “CEOs’ information security behavior in SMEs: Does ownership matter?” *Systemes d’information management*, vol. 22, no. 3, pp. 7–45, 2017.

[13] T. Gundu, “Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince,” in *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, 2019, pp. 94–102.

[14] J. Kaur and N. Mustafa, “Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME,” in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*. IEEE, 2013, pp. 286–290.

[15] S. Kabanda, M. Tanner, and C. Kent, “Exploring SME cybersecurity practices in developing countries,” *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 269–282, 2018.

[16] E. Osborn and A. Simpson, “Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study,” *The Computer Journal*, vol. 61, no. 4, pp. 472–495, 2018.

[17] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber security awareness campaigns: Why do they fail to change behaviour?” *arXiv preprint arXiv:1901.02672*, 2019.

[18] E. Osborn, “Business versus technology: Sources of the perceived lack of cyber security in SMEs,” 2015.

[19] A. Bayaga, S. Flowerday, and L. Cilliers, “IT Risk and Chaos Theory: Effect on the performance of South African SMEs,” in *WMSCI 2017 - 21st World Multi-Conference Syst. Cybern. Informatics, Proc.*, vol. 2, no. 5, 2017, pp. 48–53.

[20] B. Duncan and M. Whittington, “Enhancing Cloud Security and Privacy: The Cloud Audit Problem,” in *Cloud Computing 2016: The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization*. Rome: IEEE, 2016, pp. 119–124.

[21] B. Duncan and M. Whittington, “Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail,” in *Cloud Computing 2016: The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization*, no. April. Rome: IEEE, 2016, pp. 125–130.

[22] Y. Zhao and B. Duncan, “Could Block Chain Technology Help Resolve the Cloud Forensic Problem?” in *Cloud Computing 2018: The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization*, no. February. Barcelona, Spain: IARIA, 2018, pp. 39–44.

[23] M. Neovius, J. Karlsson, M. Westerlund, and G. Pulkkis, “Providing tamper-resistant audit trails for cloud forensics with distributed ledger based solutions,” in *CLOUD COMPUTING 2018*, 2018, p. 29.

[24] M. Westerlund, M. Neovius, and G. Pulkkis, “Providing Tamper-Resistant Audit Trails with Distributed Ledger based Solutions for Forensics of IoT Systems using Cloud Resources,” *International Journal on Advances in Security*, vol. 11, no. Number 3 & 4, pp. 223–231, 2018.

[25] M. Westerlund and M. G. Jaatun, “Tackling the cloud forensic problem while keeping your eye on the GDPR,” in *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2019, pp. 418–423.

[26] J. Wikström, M. Westerlund, and G. Pulkkis, “Smart Contract based Distributed IoT Security: A Protocol for Autonomous Device Management,” in *21st ACM/IEEE International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2021) (forthcoming)*, Melbourne, Australia, 2021.