Information Security in the Cloud: Should We be Using a Different Approach?

Bob Duncan
Computing Science
University of Aberdeen
Email: bobduncan@abdn.ac.uk

Mark Whittington
Accounting and Finance
University of Aberdeen
Email: mark.whittington@abdn.ac.uk

***Abstract*—Since the inception of cloud computing, security researchers have been active in addressing the question of cloud information security, which has seen the development of a wide range of technical solutions. The same can be said for non-cloud information security research which has been active for a far longer period of time. Yet, year on year, security breaches continue to increase, both in volume and in value. The business architecture of a company comprises people, process and technology. Is it not time to consider a different approach?**

***Keywords*—security; privacy; standards; compliance; assurance; audit; measurement; cloud service providers; service level agreements; threat environment**

I. Introduction

The goal of achieving information security is not trivial. Indeed in cloud computing, the goal is all the more challenging due to the richness and complexity of relationships between the various actors involved in cloud ecosystems. Since the inception of cloud computing, security researchers have been very active in addressing the question of cloud information security, which has seen the development of a wide range of technical solutions. This does, however, present a possible weakness in approach. Business architecture comprises people, process and technology, thus any solution ignoring people and process may potentially fail to achieve the desired result.

In earlier work with Pym [1], we developed a conceptual framework to address cloud security which takes people, process and technology into account. In this work, we identified three key barriers to good cloud security, namely standards, management method and complexity. We addressed compliance with standards [2] as well as fundamental weaknesses in that process [3], proposed management method [4], and complexity along with the difficulties in addressing measurement [5]. Having looked at our initial approach from the perspective of the company implementing the framework, we then considered the weaknesses that would still remain to be addressed. We identified the following points which will impact the successful implementation of the framework:

- Definition of security goals;
- Compliance with standards;
- Audit issues;
- Management approach;
- Complexity;
- Lack of responsibility and accountability.

We discussed these issues in our work on broadening the service level agreement (SLA)[6] where we called for better accountability from cloud service providers (CSP)s. There is no doubt that it will take time for all these issues to be properly addressed and resolved, and this introduces yet another problem: the threat environment. It is not static, it will not wait until we have proper measures in place to resist the constant onslaught of attempts to relieve us of our money. It is active now, 24/7, 365 days a year and is utterly relentless in the quest to find more victims. Thus it makes sense to turn our attention to this area.

We start by looking at research into the threat environment in Section II and in Section III we consider research into security breaches. The remainder of the paper is organized as follows: in Section IV we consider what information we can learn from security breach reports; in Section V we outline the threats which are the most pressing; In Section VI we discuss how we might go about addressing these threats; and in Section VII we discuss our conclusions.

II. The Threat Environment

The threat environment faced by cloud computing is not new. As long as computing has been around, there have been security threats against it. A great deal of work has gone into addressing this issue over many decades. Goldwasser et al [7] present a digital signature scheme based on the computational difficulty of integer factorisation. Addressing threats to information systems, Loch et al [8] report on a study investigating executives' concern about a variety of threats. A relatively new threat, computer viruses, was found to be a particular concern, and the results highlight a gap between the use of modern technology and the understanding of the security implications inherent in its use.

Torr [9] reports that even security-conscious products can fall prey when designers fail to understand the threats their software faces or the ways in which adversaries might try to attack it, and suggests the need to consider security needs throughout the design process, just as is done with performance, usability, localise-ability, serviceability, or any other facet.

Howard and Lipner [10] detail a rigorous, proven methodology that measurably minimises security bugs. The authors suggest: the use of a streamlined risk-analysis process to find security design issues before code is committed; apply secure-coding best practices and a proven testing process; conduct a final security review before a product ships; arm customers with prescriptive guidance to configure and deploy

a product more securely; establish a plan to respond to new security vulnerabilities; and integrate security discipline into agile methods and processes.

Chen et al [11] present a quantitative threat modelling method, using value driven security threat modelling based on attack path analysis. The authors demonstrate the steps of using their method to analyse the cost-effectiveness of how system patching and upgrades can improve security. Brown and Hammill [12] suggest that once it was an environmental issue, then an energy problem, and now climate change is being recast as a security threat.

Johnston and Warkentin [13] investigate the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the mitigation of threats. An examination was performed that culminated in the development and testing of a conceptual model representing an infusion of technology adoption and fear appeal theories. The authors suggest that fear appeals do impact end user behavioural intentions to comply with recommended individual acts of security, but the impact is not uniform across all end users.

Shaikh and Haider [14] aim to identify the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing. The authors' work enables researchers and security professionals to know about users' and vendors' concerns, and provide critical analysis of the different security models and tools proposed. Garvey et al [15] present a macro-analytic method for measuring economic-benefit returns on investments in cyber-security. The authors propose a mechanism which finds sets of Pareto efficient cost-benefit investments, and their economic returns, that capture tangible and intangible advantages of countermeasures that strengthen cyber-security.

Xu et al [16] present a cloud computing based system for cyber-security management and conduct extensive experiments to show the effectiveness of their developed system, and also discuss how to extend their proposed system to other applications. Shackelford et al [17] explore the Implications of the 2014 National Institute of Standards and Technology (NIST) cyber-security framework on shaping reasonable national and international cyber-security practices, and find that, given that cyber-security best practices are not yet well defined, the NIST framework has the potential to shape standards not only for critical infrastructure firms but also for the private sector, and also has the potential to shift the cyber-security landscape internationally, especially in jurisdictions that largely favour a voluntary approach to enhancing cyber-security. They further suggest that the uptake of the NIST framework beyond the US could help to foster a global standard of cyber-security care, promoting consistency, benefiting businesses active across jurisdictions, and contributing to cyber peace.

There is some variety in they types of threats which companies need to deal with. They can broadly be categorised into five types of threat: cyber espionage and terrorists; fraudsters; IT business risk; activist hackers; general criminal activity.

The threat from cyber espionage and terrorists will certainly be of concern. Often state sponsored, with a high level of technical capability and vast resources at their disposal, they will present a danger if the company is an attractive target for them. Usually industrial companies with intellectual property are a prime target for cyber espionage, particularly in aerospace, and other advanced technical industries. Critical infrastructure is generally the preferred target of the cyber terrorist, although they are not averse to stealing a bit of cash either.

The threat from fraudsters is certainly a worry, as they tend to be extremely skilled in their practices and are excellent manipulators. The threat can arise from both within the company and externally. A particular concern arises where collusion occurs between an external fraudster and company employees. Any industry which processes large volumes of cash are at risk from this type of threat. IT business risk presents an internal risk arising from a lack of understanding on the part of management, which can lead to under providing for IT business risk.

Pym et al [18] make the comment that the vast majority of businesses do not fully understand what they do, thus making it difficult to properly align IT systems to the underlying business model, which can result in the inadvertent creation of unexpected security vulnerabilities. The authors warn that there needs to be a clear understanding of the two basic needs of a control system. First, all data must include a rationale and a purpose — so that people must know why things are measured and, more importantly, what to do about them. Second, all measurement must be based on careful analysis of the business, so that the objectives of the business are linked to the things over which managers and front-line personnel have control. Only then can the recognition of a problematic measure lead to the right actions that will correct it leading to improved performance of the business as a whole.

The threat from activist hackers is an issue due to the fact that they tend to be heavily committed to their cause, and are often competent hackers. They usually target large corporates for perpetrating perceived wrongdoing (in their view), with the aim of exposing this wrongdoing. This can result in system downtime, embarrassment and regulatory fines.

The threat from general criminal activity presents the largest financial danger to companies. Some are not very sophisticated in their knowledge levels. Others are highly competent. They are out for one thing only — to line their own pockets, by continuously probing company systems until they find a weakness they can exploit. And they won't just restrict themselves to technological systems. They will be probing company employees and attempting to find out about company processes too.

Any company which fails to grasp the significance of this threat will be doing themselves a great disservice. Remember that globally, it is estimated [19] that 200,000 new pieces of malware are developed every day — that is a total of 73 million every year. All it takes is for one of these to succeed, and the consequences could be severe. Consequently, management must realise that proper security is not a technical exercise that can be devolved to the IT department. Security is a key element to the very survival of a company. Security should quite properly be a key board responsibility, with a director of sufficient experience to oversee the company approach to security.

This means that the company needs to establish effective security policies, implement proper security procedures which are driven, and enforced, from the board down, and devise adequate monitoring processes to ensure compliance. Staff training is vital for success. All it takes is for one member of staff to fall victim to a social engineering attack, or to open an infected email to expose the whole business. No matter how well trained in security practices the organisation is, security will only ever be as good as the practice of the weakest member of staff. Staff security training should also emphasise the importance of accountability, assurance, audit, confidentiality, compliance, integrity, privacy and responsibility where relevant.

Company processes are often very well documented and designed to optimise the efficiency of the organisation. All too often, security was not included on the requirements list for the processes. This presents a fundamental weakness to the security of the organisation. Where security was not on the original requirements list for company processes, they should be reviewed to establish how effective each process is from a security point of view in order to find any weaknesses in the system. These weaknesses should be identified, and changes made to improve security. All new processes being implemented should also include a security requirement. This should also be extended to cover other needs, such as accountability, assurance, audit, confidentiality, compliance, integrity, privacy and responsibility.

Companies should also regularly review their technological systems to ensure they can provide a robust defence against the threat environment. Remember, technology evolves very rapidly. So does the threat environment. It is not static. It dynamically changes day by day. As soon as a new vulnerability is found, software developers race to find a solution. As soon as patches are released, the bad guys race to counter the patch. And so the vicious circle continues. Companies need to keep on top of vulnerabilities and patch them promptly. Many companies only update software once or twice a year. By the time the next update comes along, the weaknesses may have already been found and exploited by the bad guys. There may not be any systems to update by the time the next update is due. That is how serious a breach can be.

III. Security Breach Research

Pym et al [18], in discussing the quest of alignment of IT to business needs, warn that there needs to be a clear understanding of the two basic needs of a control system. First, all data must include a rationale and a purpose — so that people must know why things are measured and, more importantly, what to do about them. Second, all measurement must be based on careful analysis of the business, so that the objectives of the business are linked to the things over which managers and front-line personnel have control. Only then can the recognition of a problematic measure lead to the right actions that will correct it leading to improved performance of the business as a whole.

Davis et al [20] report on two types of empirical research conducted on cyber security breaches. In the first, where they review reporting of cyber security incidents, they find that the likelihood of a cyber security incident being reported in specialised press increases with the total number of affected customers, the company breached being publicly traded and whether or not commercially sensitive information was lost. In the second, where they considered security incidents for mainly on-line businesses, they find that such incidents do not affect the overall web traffic for such businesses.

Armbrust et al [21] provide a detailed review and explanation of cloud computing, expressing concern over the increase in security issues. They discuss how responsibilities need to be properly addressed between the various actors involved, in order to mitigate the effect of security breaches, both from within the cloud, and externally. Blandford [22] discusses the reluctance of business to take up cloud computing, citing concern over potential security issues, outlining many of the dangers with the cloud, endorsing the use of standards to ensure security.

Monfared and Jaatun [23] review existing security monitoring mechanisms and highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them, but recognise the field of cloud security is not yet mature. Gordon et al [24] carry out a study on the effect of information security breaches on market returns of firms. Opara and Bell [25] investigate stiffening access to sensitive data, and found no difference in the reported cases of breaches on having a formal IT policy, external access from mobile devices, and number of times clients were required to change their passwords, regardless of the security protocol.

Wenge et al [26] warn of the dangers involved where the lack of capacity, unplanned outages of sub-contractors, a disaster recovery plan, acquisitions, or other financial goals may force cloud providers to enter into collaborations with other cloud providers. However, they explain that the cloud provider is not always fully aware of the security level of a potential collaborative cloud provider, which can lead to security breaches and customers' data leakage, ending in court cases and financial penalties. They analyse different types of cloud collaborations with respect to their security concerns and discuss possible solutions, and outline trusted security entities as a feasible approach for managing security governance risks and propose their security broker solution for ad hoc cloud collaborations. Armerding [27] describes the 15 worst data security breaches of the 21st century.

There is a move to consider privacy in the healthcare arena. Kwon and Johnson [28] explore information security practices and identify practice patterns that are associated with improved regulatory compliance in healthcare, providing security practice benchmarks for healthcare administrators which can help policy makers in developing strategic and practical guidelines for practice adoption. Taitsman et al [29] investigate protecting patient privacy and data security in healthcare, identifying a number of key areas of weakness.

Gordon et al [30] examine how the existence of well-recognised externalities changes the maximum a firm should, from a social welfare perspective, invest in cyber security activities. By extending their cyber security investment model to incorporate externalities, the authors show that the firm's social optimal investment in cyber security increases by no more than 37% of the expected externality loss. Renaud and Goucher [31] investigate the curious incidence of security

breaches by knowledgeable employees and the pivotal role a of security culture in achieving better protection. Watkins [32] prepares a report on the impact of cyber attacks on the private sector for the Association for International Affairs, and warns of the ever increasing threat level posed by cyber attacks.

Chou [33] analyses the risk and value components inside cloud computing practice through a value creation model. Garg and Camp [34] examine information security risk communication, which struggles with the challenges of explaining ever evolving technology and corresponding risks to a non-technical user base. The authors examine the relevance of nine canonical characteristics of risk in explaining perceived risk online, across five distinct mental models of risk communication employed by security experts. They find that severity of consequences, as well as whether the risk impacts one individual at a time or several individuals at once, are the predominant characteristics that inform risk perception of security risks, irrespective of the mental model of risk communication.

IV. Security Breach Reports

A number of specialist security firms, such as Cisco [35], Kaspersky [36], Microsoft [37], PWC [38], Symantec [39], Trend [40], Trustwave [41] and Verizon [42], have maintained an active interest in security breaches, and publish annual reports on their findings.

We look at the top threats reported by two of these companies during the period from 2010 to 2014. First, we chose Verizon in TABLE I, since their analysis includes not only their own figures, but includes figures provided by some 50 other organisations, including computer emergency response teams (CERT)s, cyber centres, forensic providers, information security (INFOSEC) product and service providers, information sharing and analysis centres (ISAC)s and law enforcement agencies. These reports provide a useful perspective on the global impact of the threat environment.

Threat	2010	2011	2012	2013	2014
Hacking	2	1	1	1	1
Malware	3	2	2	2	2
Misuse by company employees	1	4	5	5	5
Physical theft or unauth. access	5	3	4	3	4
Social Engineering	4	5	3	4	3

TABLE I. Verizon Top 5 Security Breaches — 2010-2014 (1=Highest) [43][44][45][46][47]

It is interesting to see that hacking, malware and social engineering have continued to maintain a high position in the chart. Clearly, criminals persist in using techniques which work. While misuse by employees was initially the worst threat in 2010, it quickly fell to bottom position for the following years. In comparing this with the findings from 1992 [8], at that time, hacking was considered the 7th worst threat, malware was the 6th worst threat, and social engineering hadn't been heard of as a threat yet. The second reports we selected were those from Price Waterhouse Cooper in TABLE II, which were prepared for the UK government's Department for Business, Innovation and Skills, which provides us with a perspective on the UK threat situation. These reports were historically prepared every second year, although the information is now available annually.

Threat	2010	2011	2012	2013	2014
Hacking	2	N/a	2	2	1
Malware	3	N/a	3	3	3
Misuse by company employees	1	Na	1	1	2
Physical (theft or unauthorised access)	4	N/a	4	4	4

TABLE II. PWC/BIS Top 4 Security Breaches — 2010-2014 (1=Highest) [48][49][50][51]

While it is interesting to see that hacking and malware mirrors the trend seen in the Verizon reports, misuse by employees remains a consistently high threat to UK businesses. In their latest breach report, Verizon [52] report the three most favoured attack vectors are email attachments, email links and web drive-by infections which account for 93.9% of all successful attack vectors deployed today [52].

Companies need to use every possible resource available to them in the fight against security breaches. Regular analysis of freely available security breach reports will provide a clear view of what the most serious current threats are to allow them to better assess their defences.

V. The Most Pressing Threats

It is clear that on the internal side, of the three business architecture elements of people, process and technology, the greatest threat remains people. Process remains a concern and while much good research on technical solutions has limited the impact of technological threats on companies, this still remains an issue. From the external side, hacking and malware continue to pose a serious threat, with social engineering continuing to find a place in the threat armoury.

The use of email attachments, email links and web drive-by infections as a means of delivering threats is very concerning, since these threats are not overly technically challenging to resolve. Yet they remain the preferred attack vector of choice for a reason — they continue to be successful, year on year. These threat vectors apply across all companies, whether large or small, and a little effort could go a long way to mitigating these attacks.

Of course, for the larger companies, a more concerning issue is the increase in advanced persistent threats (APT)s and targeted attacks. These are more worrying, because these types of attack tend to be perpetrated by adversaries who have much greater technical competence and resources at their disposal. Many are state-sponsored, but hacktivists, who can be very competent and determined, also can fall into this category. Compromise from these attacks can be far more costly to the business, and far more difficult and expensive to resolve.

Yet rather worryingly, the average time between compromise and discovery can be over 200 days [52]. In the company security threat model shown in Fig. 1 below, we can see how the different threat vectors are used against a company. As we can see from the previous section, it is a worry that the top three attacks against people account for 93.9% of all successful attacks.

VI. How to Address These Current Threats

Back in 2002, Gordon and Loeb [54] developed an economic security model to determine the optimum amount companies should spend on information security, noting that many

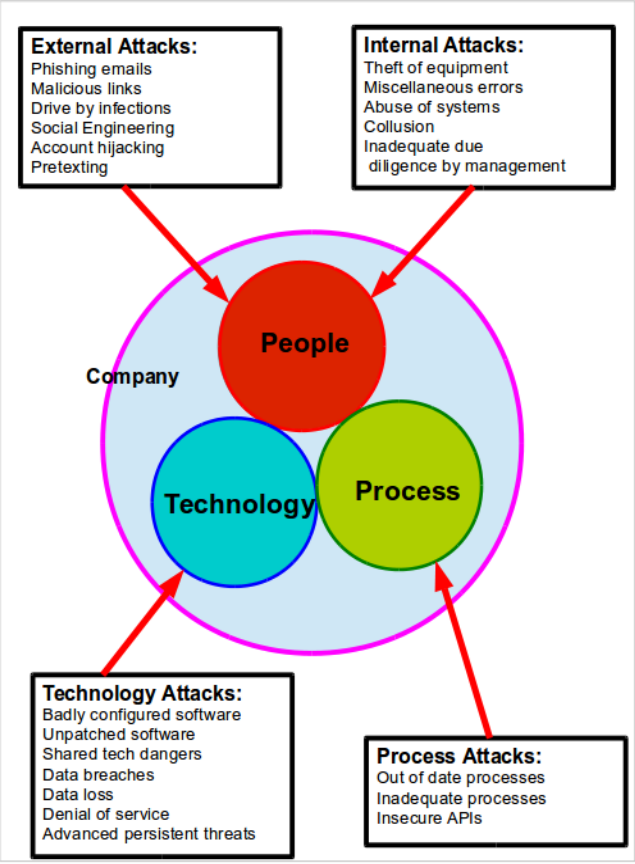

Fig. 1. A Company Security Threat Model

companies often spent far more than they needed to, and often on the wrong areas to optimise their return on investment.

In 2008, the National Institute of Standards and Technology (NIST) [55] published a guide for mapping types of information and information systems to security categories, in which they took a risk based approach to security. One of the key elements of this guide was the trade-off between criticality and sensitivity. NIST define criticality as: "a measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function"; and sensitivity as: "used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection". We can usefully apply these principles in any approach to achieving better security for optimal cost.

People are likely to be the weakest link in companies and continue to present a danger to their security, not just from misuse but also from naïvety of behaviour. Better, continuing education can certainly help here. This education should concentrate on the key areas of risk, and how to mitigate the impact of these threat vectors.

Developing a good security culture within the organisation is always a positive step, although it may be necessary to motivate some employees through penalties for consistent abuses of security policy. Companies should carry out regular reviews of their processes to ensure they are, or remain, secure, updating as necessary to reflect emerging trends. All company systems should be reviewed for security regularly in the light of the evolving threat environment, ensuring security patches are updated regularly.

As to the serious threats posed by the favoured attack vectors, a simple policy change could present an effective improvement overnight for minimal cost. Automatic deletion of attachments from unknown email users could be implemented simply at a systems level to remove this threat quickly.

Similarly, stripping email links from unknown email users could be effected very simply at a systems level. Implement a validation procedure for all incoming email messages is another option that could be used to filter out unwanted traffic. In the longer term, some technical changes to email software could be developed to validate properly the true source of all email traffic, with automatic deletion of traffic failing the test. Better restriction could be introduced to ensure employees do not access questionable web sites, thus minimising the impact of drive-by infections.

VII. Conclusion

So what is the answer to the question, should we be using a different approach? Rather annoyingly, the answer is both no, and yes. Current approaches, which are usually highly technical in nature, are a response to the increasingly complex nature of information security in the cloud. We must necessarily continue with this approach to ensure that increasing technical complexity does not create new vulnerabilities for those with criminal intent to exploit, so the answer here is no. However, it is also clear that many of the simplest vulnerabilities are being ignored, thus leaving systems greatly exposed to exploitation, and thus our answer must be yes.

Thus it is clear that the research community needs to remember to consider that many of the more simple threats remain a serious problem. As noted in Section IV above, just three very familiar approaches — the use of email attachments, email links and web drive-by infections account for 93.9% of all successful attacks. Simple threats can often provide a valuable return on investment to address. While they might be less intellectually challenging than many of the more technical issues being worked on today, nevertheless some attention to this area could have a meaningful impact on lowering the cost of security breaches.

References

[1] B. Duncan, D. J. Pym, and M. Whittington, "Developing a Conceptual Framework for Cloud Security Assurance," in *Cloud Comput. Technol. Sci. (CloudCom), 2013 IEEE 5th Int. Conf. (Volume 2)*. Bristol: IEEE, 2013, pp. 120–125.

[2] B. Duncan and M. Whittington, "Compliance with Standards, Assurance and Audit: Does this Equal Security?" in *Proc. 7th Int. Conf. Secur. Inf. Networks*. Glasgow: ACM, 2014, pp. 77–84.

[3] B. Duncan and M. Whittington, "Reflecting on Whether Checklists Can Tick the Box for Cloud Security." in *Cloud Comput. Technol. Sci. (CloudCom), 2014 IEEE 6th Int. Conf.* Singapore: IEEE, 2014, pp. 805–810.

[4] B. Duncan and M. Whittington, "Company Management Approaches Stewardship or Agency: Which Promotes Better Security in Cloud Ecosystems?" in *Cloud Comput. 2015*. Nice: IEEE, 2015, pp. 1–6.

[5] B. Duncan and M. Whittington, "The Importance of Proper Measurement for a Cloud Security Assurance Model," forthcoming in *Cloud Comput. Technol. Sci. (CloudCom), 2015 IEEE 7th Int. Conf. Vancouver: IEEE, 2015.*

[6] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement," in *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15)*. Helsinki, Finland, 2015.

[7] S. Goldwasser, S. Micali, and R. L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, 1988.

[8] K. D. Loch, H. H. Carr, M. E. Warkentin, and H. H. Carr, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Q.*, vol. 16, no. 2, pp. 173–186, 1992.

[9] P. Torr, "Demystifying the threat modeling process," *IEEE Secur. Priv. Mag.*, vol. 3, pp. 66–70, 2005.

[10] M. Howard and S. Lipner, "The Security Development Lifecycle," *Change*, vol. 34, no. May, p. 352, 2006.

[11] Y. Chen, B. Boehm, and L. Sheppard, "Value driven security threat modeling based on attack path analysis," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 280a–280a, 2007.

[12] O. L. I. Brown and A. Hammill, "Climate Change as the 'New' Security Threat: Implications for Africa," *Int. Aff.*, vol. 83, no. 6, pp. 1141–1154, 2007.

[13] B. A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Q.*, vol. 34, no. 3, pp. 549–566, 2010.

[14] F. B. F. Shaikh and S. Haider, "Security threats in cloud computing," in *2011 Int. Conf. Internet Technol. Secur. Trans.*, no. December, 2011, pp. 214–219.

[15] P. R. Garvey, R. A. Moynihan, and L. Servi, "A Macro Method for Measuring Economic-Benefit Returns on Cybersecurity Investments: The Table Top Approach," *Syst. Eng.*, vol. 16, no. 3, pp. 313–328, 2013.

[16] G. Xu, W. Yu, Z. Chen, H. Zhang, and P. Moulema, "A cloud computing based system for cyber security management," *Int. J. Parallel, Emergent Distrib. Syst.*, vol. 30, no. 1, pp. 29–45, 2015.

[17] S. Shackelford, A. Proia, B. Martell, and A. Craig, "Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices," *Tex. Int. Law J.*, no. 291, pp. 1–58, 2015.

[18] D. Pym, R. Taylor, and C. Tofts, "Public services innovation through technology," in *Manag. Eng. Technol. Portl. Int. Cent.*, 2007, pp. 2736–2739.

[19] Kaspersky, "Global Corporate IT Security Risks: 2013," Tech. Rep. May, 2013.

[20] G. Davis, A. Garcia, and W. Zhang, "Empirical analysis of the effects of cyber security incidents," *Risk Anal.*, vol. 29, no. 9, pp. 1304–16, Sep. 2009.

[21] B. Armbrust, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A View of Cloud Computing," *Commun. ACM*, vol. 53, no. 4, pp. 50—-58, 2010.

[22] R. Blandford, "Information security in the cloud," *Netw. Secur.*, vol. 2011, no. 4, pp. 15–17, 2011.

[23] A. T. Monfared and M. G. Jaatun, "Monitoring intrusions and security breaches in highly distributed cloud environments," *Proc. - 2011 3rd IEEE Int. Conf. Cloud Comput. Technol. Sci. CloudCom 2011*, no. Section 3, pp. 772–777, 2011.

[24] L. a. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?" *J. Comput. Secur.*, vol. 19, pp. 33–56, 2011.

[25] E. U. Opara and R. L. Bell, "The Relative Frequency of Reported Cases by Information Technology Professionals of Breaches on Security Defenses," *Int. J. Glob. Manag. Stud. Prof.*, vol. 3, no. 2, pp. 15–29, 2011.

[26] O. Wenge, M. Siebenhaar, U. Lampe, D. Schuller, and R. Steinmetz, "Much Ado about Security Appeal: Cloud Provider Collaborations and Their Risks," *Serv. Cloud Comput.*, vol. 7592, no. 1, pp. 80–90, 2012.

[27] T. Armerding, "The 15 worst data security breaches of the 21st century," *CSO online*, no. March 2011, p. 4, 2012.

[28] J. Kwon and M. E. Johnson, "Security practices and regulatory compliance in the healthcare industry," *J. Am. Med. Informatics Assoc.*, vol. 20, no. 1, pp. 44–51, 2013.

[29] J. K. Taitsman, C. M. Grimm, and S. Agrawal, "Protecting Patient Privacy and Data Security," *N. Engl. J. Med.*, no. 14 Mar 2013, pp. 977–979, 2013.

[30] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model," *J. Inf. Secur.*, vol. 6, no. January, pp. 24–30, 2014.

[31] K. Renaud and W. Goucher, "The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture," in *Hum. Asp. Inf. Secur. Privacy, Trust*, 2014, pp. 361–372.

[32] B. Watkins, "The Impact of Cyber Attacks on the Private Sector," Association for International Affairs, Tech. Rep. August, 2014.

[33] D. C. Chou, "Cloud computing: A value creation model," *Comput. Stand. Interfaces*, vol. 38, pp. 72–77, 2015.

[34] V. Garg and L. J. Camp, "Risk Characteristics, Mental Models, and Perception of Security Risks," *Acad. Sci. Eng. USA*, pp. 1–10, 2015.

[35] Cisco, "Cisco," 2015. [Online]. Available: http://www.cisco.com/

[36] Kaspersky, "Kaspersky," 2015. [Online]. Available: http://www.kaspersky.co.uk/

[37] Microsoft, "Microsoft," 2015. [Online]. Available: https://www.microsoft.com

[38] PwC, "The Global State of Information Security," PwC, Tech. Rep., Jan. 2015.

[39] Symantec, "Symantec," 2015. [Online]. Available: http://www.symantec.com/

[40] TrendMicro, "TrendMicro," 2015. [Online]. Available: http://www.trendmicro.co.uk/

[41] Trustwave, "Trustwave," 2015. [Online]. Available: https://www.trustwave.com

[42] Verizon, "Verizon," 2015. [Online]. Available: http://www.verizon.com/

[43] Verizon, "2010 Data Breach Investigation Repeort: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service," Verizon/USSS, Tech. Rep., 2010.

[44] Verizon, "2011 Data Breach Investigation Repeort: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others," Verizon/USSS, Tech. Rep., 2011.

[45] Verizon, "2012 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others," Tech. Rep., 2012.

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

[47] Verizon, "2014 Data Breach Investigations Report," Tech. Rep. 1, 2014.

[48] PWC, "Information Security Breaches Survey 2010 Technical Report," PWC, London, Tech. Rep., 2010.

[49] PWC, "UK Information Security Breaches Survey - Technical Report 2012," PWC2012, Tech. Rep. April, 2012.

[50] PWC, "Key findings from The Global State of Information Security Survey 2013," Tech. Rep., 2013.

[51] PWC, "2014 Information Security Breaches Survey," Tech. Rep., 2014.

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

[53] Verizon, "Threat Delivery Vectors," Tech. Rep., 2015.

[54] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, Nov. 2002.

[55] NIST, "SP 800-60 Volume I Rev1: Guide for Mapping Types of Information and Information Systems to Security Categories," Tech. Rep. August, 2008.