Basic Cyber Hygiene: Does it work?

Jose M. Such
King's College London

Pierre Ciholas
Lancaster University

Awais Rashid
University of Bristol

John Vidler
Lancaster University

Timothy Seabrook
University of Oxford

The resources required to establish and maintain cyber security often results in Small and Medium Enterprises (SMEs) being left unprotected, risking not just their own but also the supply chain of other larger organisations. A number of security certifications for SMEs have been proposed, but how effective are these schemes? We conducted the first effectiveness evaluation of one such scheme, Cyber Essentials, and found that its security controls seem to work well to mitigate the threats they were designed for, i.e., those threats exploiting vulnerabilities remotely with commodity-level tools. The results may also be applicable to other schemes for SMEs around the globe that share/include the same security controls.

KEYWORDS: Cyber Hygiene, SME security, SMB security, Security Controls, Security Standards.

Small to Medium Enterprises (SMEs) – also known as Small to Medium Businesses (SMBs) – constitute a very important, yet sometimes underestimated, part of the economy around the globe. For instance, in the US, of the 5.68 million employers, SMEs accounted for over 99% of all enterprises [1], and in Europe as a whole, 99% of approximately 23 million companies are SMEs [2]. The Internet has facilitated many of these SMEs with the means to connect with a larger audience, expanding their market reach - but has also exposed their operations to risks from cyber-threats. While larger organisations will often have pre-allocated resources to combat and maintain security in the face of cyber-attacks, the additional focus and resources required in order to establish and maintain a secure on-line presence often results in SMEs being left unprotected. For instance, in 2017 approx. 49% of SMEs suffered an attack in the UK in 2017 [3], and around 61% of SMEs suffered a cyber-attack in the US [4]. In addition, SMEs are often part of the supply chain of larger organisations, therefore being a security risk not just for their own, but also for their customers' and partners' data and security. There are multiple examples of organi-

sations having been attacked by compromising other organisations in their supply chain, such as the infamous Target and Home Depot breaches [5] as well as the Stuxnet attack [6].

There have been some *low-cost* initiatives aimed to improve the cyber security of SMEs. These initiatives include a subset of the security controls considered by schemes and frameworks for larger organisations, such as the very well-known and widely used ISO27000-series and the Centre for Internet Security (CIS) Critical Security Controls. Examples of these low-cost initiatives for SME include several good practices and guidance around the globe [7], such as the US NIST NISTIR-7621 "Small Business Information Security: the fundamentals", the Belgian Cyber Security Guide, and the French CGPME/ANSSI "Guide Des Bonnes Practiques De L'Informatique"; and assurance schemes such as UK Cyber Essentials [8]. However, and to the best of our knowledge, there is a lack of systematic evaluation of the effectiveness of such initiatives. Yet such schemes are becoming mandatory. Cyber Essentials was made mandatory for all suppliers of UK government contracts involving "*the handling of sensitive and personal information and provision of certain technical products and services*" [9]. Large private sector companies also require it for their supply chain, such as Hewlett-Packard (HP) in the UK requiring Cyber Essentials for its entire supply-chain (≈ 600 SMEs) [10]. The need for a systematic evaluation of the effectiveness of such schemes is becoming even more important given the almost regulatory nature that such schemes are acquiring.

We conducted the first effectiveness evaluation of one such scheme, Cyber Essentials. We found that Cyber Essentials security controls work well in the SMEs we studied to mitigate the threats these security controls were designed for, i.e., those threats exploiting vulnerabilities remotely with commodity-level tools, completely mitigating around 2/3 of this type of vulnerabilities, partially mitigating almost a further 1/3, with only very few immitigable vulnerabilities. Although we focus on Cyber Essentials, the results may also be applicable to other schemes for SMEs like the examples above from NIST, ANSSI, and Belgium, as they include all or most of the Cyber Essentials security controls.

(TO GO AS SIDEBAR) RELATED WORK ON SME SECURITY

Very few previous works have considered SME / SMB security with notable exceptions including the following.

Some works focused on the acceptance, suitability and the feasibility of the use in practice of well-known information security standards by SMEs. For instance, [11] showed that applying ISO 27001 to medium-sized enterprises led to many of the requirements of the standard being unattainable. This confirms other studies that have pointed out that general-purpose information security standards like ISO 27001 face many barriers to be applied in SMEs, including lack of skilled resources, time needed to apply it, the complexity of the standard, the cost of the process of certification, and a clear quantification of the benefits of applying them [12].

Other works focused on studying and understanding the security culture of SMEs. For instance, [13] showed that SME owners lacked an understanding of the strategic value of IT to their business and security technologies were viewed as business costs rather than strategic enablers. They also highlighted the need for the development of special information security risk assessment standards tailored to SMEs.

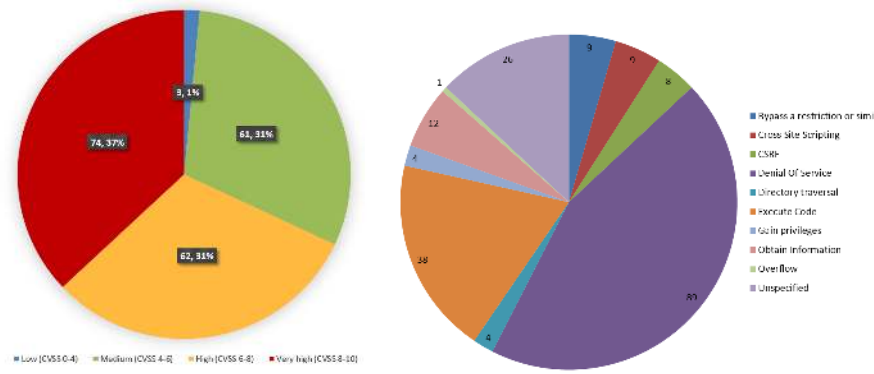
More recently, [14] presented an abstract model to calculate the indirect costs of deploying security controls based on Cyber Essentials in (SMEs). However, to date, no work has studied the effectiveness of security controls in standards and guidelines specifically tailored to SMEs.

CYBER ESSENTIALS

In brief, the Cyber Essentials security controls can be summarised as follows [8]: 1) *Firewalls and Gateways* to prevent unauthorised access to or from private networks; 2) *Secure Configuration* to ensure that systems are configured in the most secure way for the needs of the organisa-

tion; 3) *Access Control* to ensure only those who should have access to systems to do so at the appropriate level; 4) *Malware Protection* to ensure virus and malware protection is installed and is it up to date – including *website blacklists*; and 5) *Patch Management* to ensure the latest supported version of applications is used and all the necessary patches supplied by the vendor has been applied. Other schemes for SME around the globe recommend security controls similar to those included in Cyber Essentials. For instance, NISTIR-7621 includes, among others, the 5 security controls of Cyber Essentials, and the Belgian and the CGPME/ANSSI schemes include some form of Patch Management, Malware Protection, Secure Configuration, and Access Control – refer to [7] for a detailed analysis of these schemes and Cyber Essentials, together with their commonalities and differences.

The security controls of Cyber Essentials and similar schemes are particularly aimed at providing a basic level of cyber security that is as cheap to implement as possible, yet they should defend against remotely-exploitable commodity-level vulnerabilities [15]. Therefore, in order to evaluate to what extent these security controls actually defend against this type of vulnerabilities we *randomly* chose 200 vulnerabilities shown by severity and type in Figure 1 from the CVE database [16] for the two years preceding 2015, which was the most recent data on vulnerabilities available when the vulnerability collection was carried out, amounting to a total of 10,488 vulnerabilities. As we use random sampling, this means that, with a 95% confidence interval, the results we obtained may be generalised to that total amount with an error of +/- 6.9% [17]. The severity and type of each vulnerability was obtained for each CVE vulnerability using the standard Common Vulnerability Scoring System (CVSS) [18].



(a) Vulnerability Severity. (b) Vulnerability Type.

Figure 1: Severity and Type of the 200 *Randomly* Selected Vulnerabilities.

To conduct the vulnerability assessment and assess the effectiveness of the 5 cyber essentials security controls, and due to the nature of SMEs that do not have the resources to separate testing from operational systems, we sought to avoid "active" security testing techniques like penetration testing, which may have an operational impact on this already resource-constrained type of businesses. Instead, we used a less aggressive approach, particularly using: architectural reviews, configuration reviews, and interviews, which are, however, known to be some of the most cost-effective security testing techniques in practice [19]. As part of the assessment, we firstly mapped between the selected SME's characteristics (see below) and network features on the one hand and the 200 randomly selected vulnerabilities on the other hand. We looked at the specific hardware, software used, and organisational practices and policies to determine if a vulnerability would be applicable to each SME, using the information elicited during the architectural and configuration reviews and interviews. Then, a double-vetted, i.e., two researchers working independently from each other, process of mitigation assessment was conducted considering the applicable vulnerabilities and whether the vulnerabilities would be mitigated or not if the security controls were implemented in the SMEs.

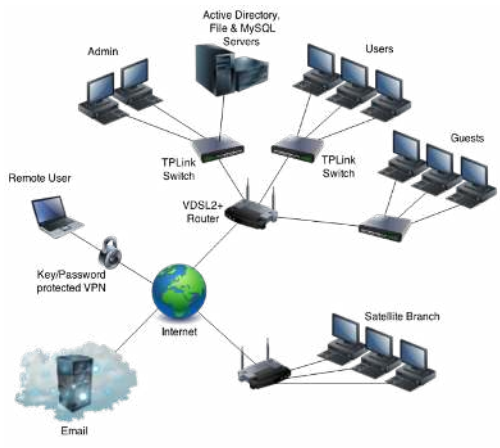
Case Studies

The SMEs we studied represent organisations from a range of market sectors, from finance (SME 1), to specialist scientific services (SME 2), to web development and online presence (SME 3), and to hospitality services (SME 4). We conducted a wider survey to ensure the 4 SMEs were representative of the SME sector in terms of their characteristics and IT systems – the total number of SMEs surveyed was 20 (for a full breakdown of the survey questions refer to [20]). In particular, Table 1 contrasts the 4 SMEs selected with the 20 SMEs surveyed. The darker the colour in the "Survey" column, the higher the proportion of the 20 SMEs claiming to have these characteristics, with white meaning none and black meaning all of them. We can see that the 4 SMEs we selected are at the same time representative of a range of different characteristics to maximise variety, but they also cover all the characteristics with a darker colour, which were predominant and most prevalent in the 20 SMEs surveyed. Importantly, the predominant characteristics of the 20 SMEs surveyed match the results obtained in larger surveys like [3] (which included over 1,300 SMEs), though these larger surveys included less characteristics, but those included largely match our results (e.g. BYOD, third-party services, etc.). However, this does not mean that the results we obtained for the 4 SMEs we studied in detail are completely generalisable to all SMEs, and any generalisations from our research should be made with care. Table 1 shows a breakdown of the main characteristics and services of the SMEs with their network diagrams shown in Figure 2.

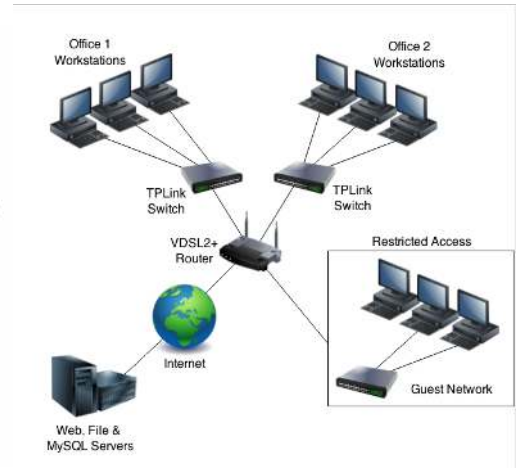
Table 1: Main Characteristics and Services of the SMEs studied.

		Survey	SME1	SME2	SME3	SME4
Employees	1-10 (small)				*	*
	11-250 (small-to-medium)		*	*		
WorkStations	Windows 7/8		*	*	*	*
	Windows (older)			*		
	OSX			*	*	*
	Linux					
Bring Your Own Device	Yes			*	*	*
	No		*			
Local Services	File Sharing/Server		*	*	*	
	Database		*			
	Email					
	Domain Server		*			
	Webserver		*			
	Application Server		*			
OS for Local Services	Windows		*	*	*	
	OS X					
	Linux		*			
3rd Party	Email		*	*	*	*

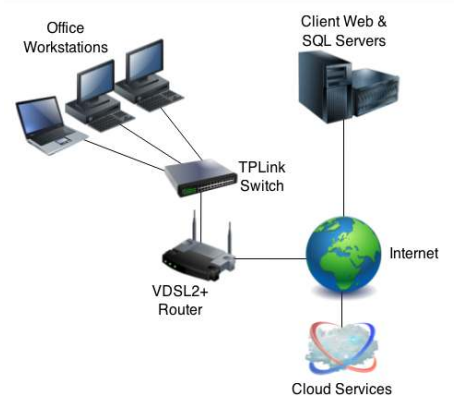
Remote Services	Web Hosting			*		*
	Online Banking / Accounting		*			*
	Social Media					
	File Sharing (e.g. dropbox)			*	*	*
	Data (e.g. Web Database)			*	*	*
Remote access to local services	Not Permitted				*	*
	Connect to Network (e.g. VPN)		*	*		
	Connect to Server (e.g. SSH)					



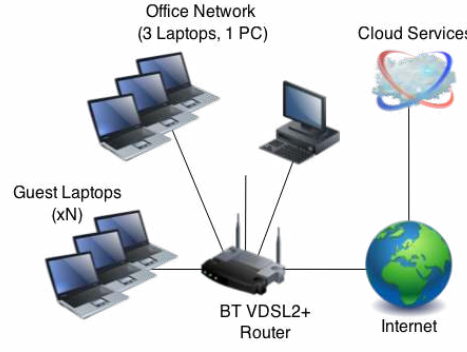
(a) SME 1 – Finance Sector.



(b) SME 2 – Specialist Group.



(c) SME 3 – Web Development.



(d) SME 4 – Hotel Services.

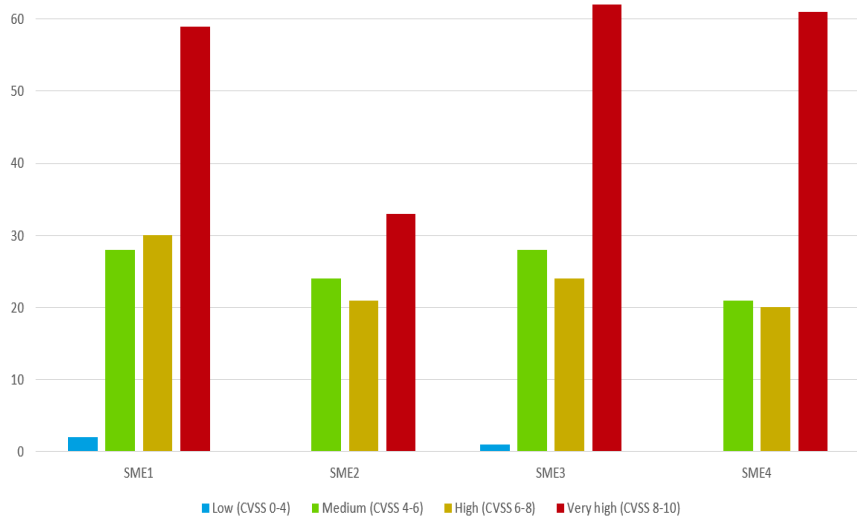
Figure 2: Network Diagrams

MAIN FINDINGS

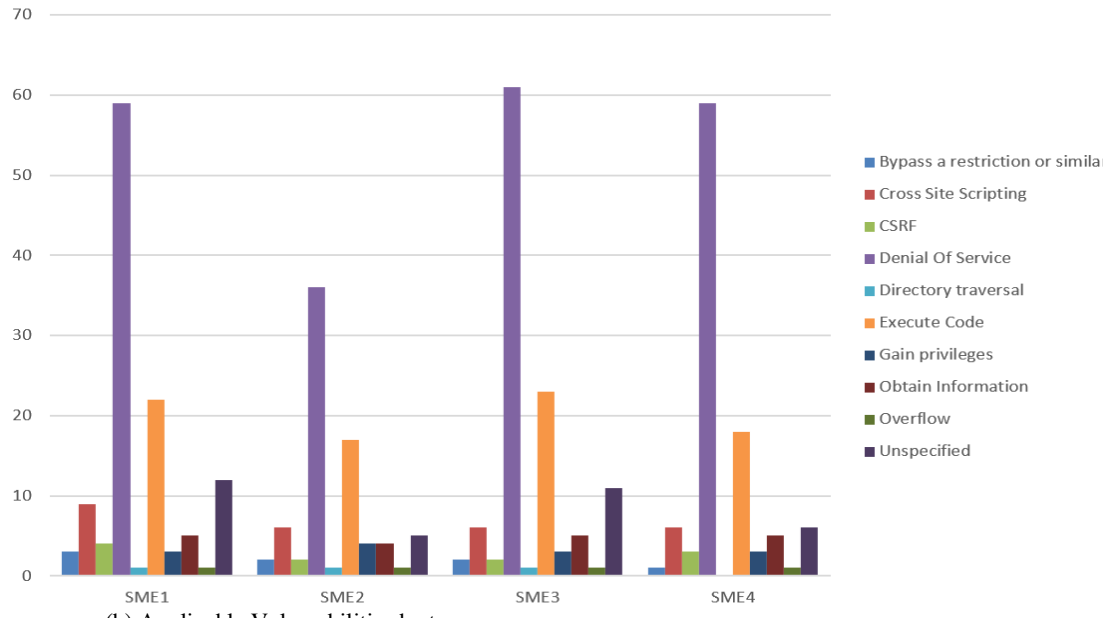
Applicable Vulnerabilities not only depend on network/service complexity

From the 200 randomly selected vulnerabilities, following the method stated above, 137 in total were applicable to at least one SME (with 63 out of the 137 applicable to all SMEs), which clearly suggests that SMEs are indeed very vulnerable. In particular, we can observe in Figure 3.a that in all SMEs, very high-risk vulnerabilities (according to their CVSS rating) largely dominate. This can be partially explained by figure 3.b, which reveals that the most common types of vulnerabilities are Denial of Services, Code Execution and Gaining Privileges.

When looking at each individual SME, Figure 3 shows SME 1 in the first place in terms of the number of applicable vulnerabilities, which is mainly due to the more complex network and also the high number of local services offered, together with the use of both Windows and Linux (see Table 1). However, *applicable vulnerabilities and, in particular, their severity do not only depend on the complexity of the network and the services offered*. Indeed, when we observe the results for SME 3 and SME 4, they seem counter-intuitive. They have a simpler network and fewer local services running than SME 2 and SME 1, and yet they have more applicable vulnerabilities than SME 2, with even a few more very high-risk ones than SME 1. This has indeed a number of explanations beyond the complexity of the network diagram. For instance, SME 3 (web development) have the business requirement that everything they develop should operate across multiple web browsers on various versions to test and build a customer's website, which means they accumulate all vulnerabilities in all these different web browsers. In SME 4, guests have no restrictions placed on their network usage, and naturally may bring their own equipment providing a mix of all operating systems currently available, including Windows, Linux, Mac among others. Therefore, the actual business requirements also play a very important role in determining the attack surface. Indeed SME 1, SME 3, and SME 4 are rather different from each other, but they have a similarly large attack surfaces, even though the specific vulnerabilities that may be exploited in each case are not necessarily the same.



(a) Applicable Vulnerabilities by Severity

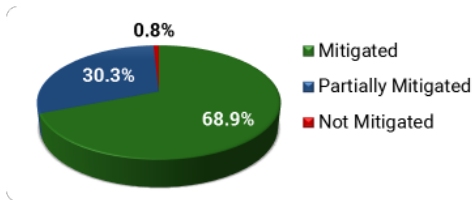


(b) Applicable Vulnerabilities by type

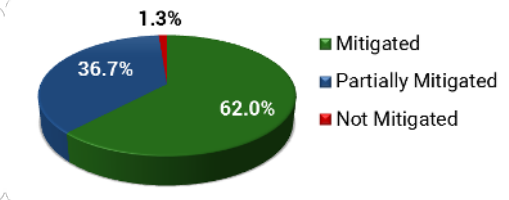
Figure 3: Applicable Vulnerabilities for each SME.

Getting the basics right matters a great deal

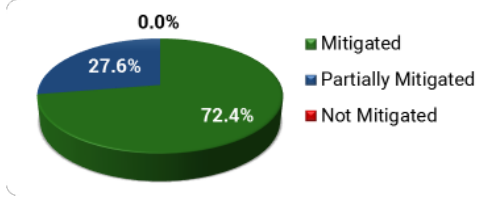
From the 137 vulnerabilities that were applicable to at least one of the SMEs studied, 95 (69.3%) were mitigated with the use of the Cyber Essentials security controls, 40 (29.2%) were partially-mitigated, and 2 (1.5%) were not mitigated – for a full table with a detailed analysis per each individual CVE vulnerability against each of the 4 case studies, we refer the reader to our technical report [20]. Figure 4 shows that these figures are similarly positive across the 4 SMEs, with at most 72% (SME 3) and at least 62% (SME 2) of all the applicable vulnerabilities *fully mitigated*. Therefore, there was a similar proportion of vulnerability mitigation regardless of the particular SME. There is also around a quarter of vulnerabilities for which cyber essentials security controls would *partially mitigate* the vulnerability – more details about partially-mitigated vulnerabilities later on.



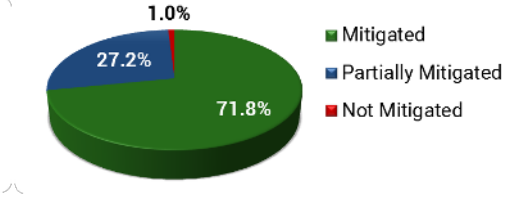
(a) SME 1 – Finance Sector.



(b) SME 2 – Specialist Group.



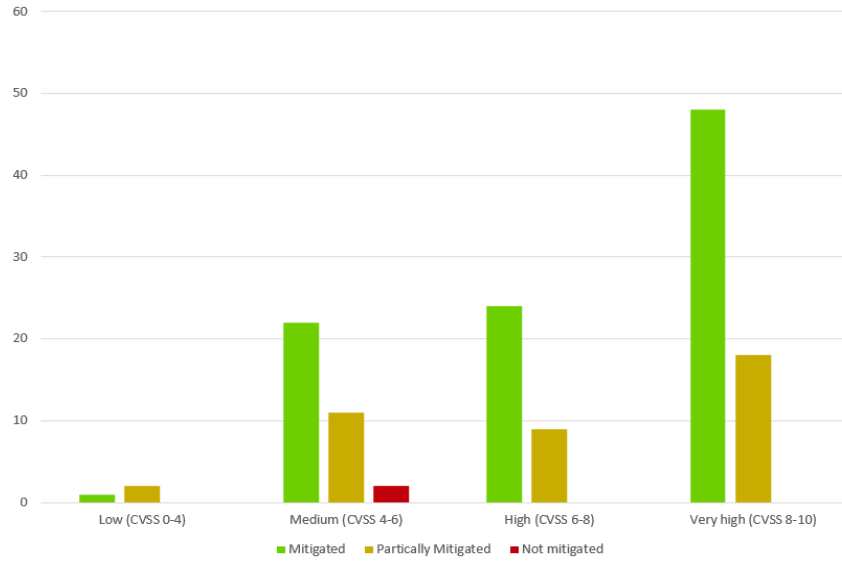
(c) SME 3 – Web Development.



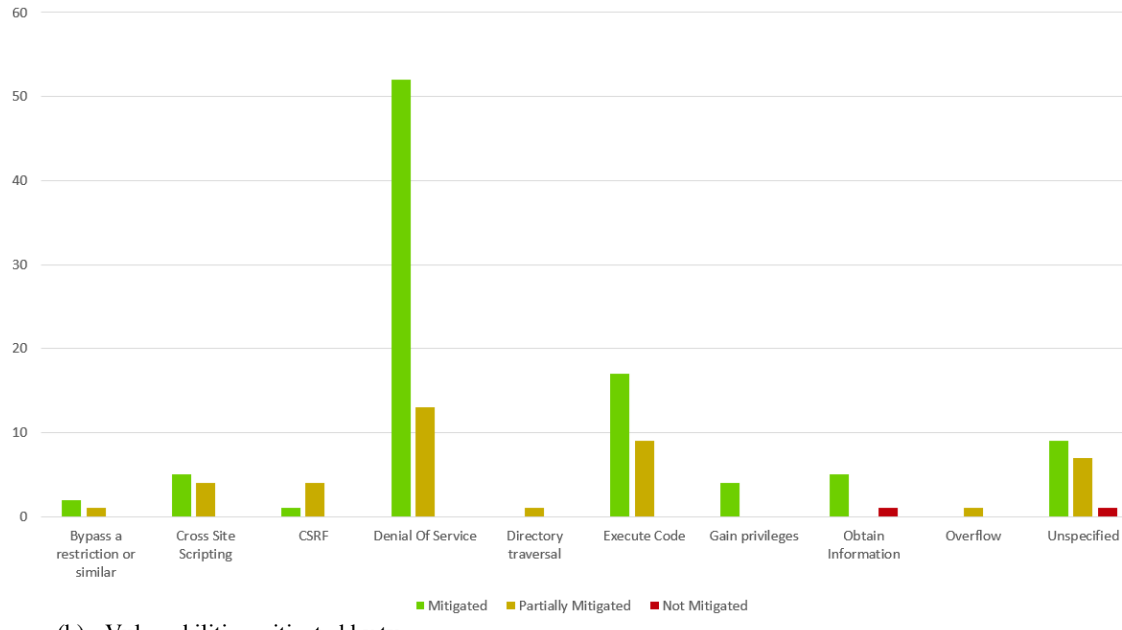
(d) SME 4 – Hotel Services.

Figure 4: Vulnerability Mitigation

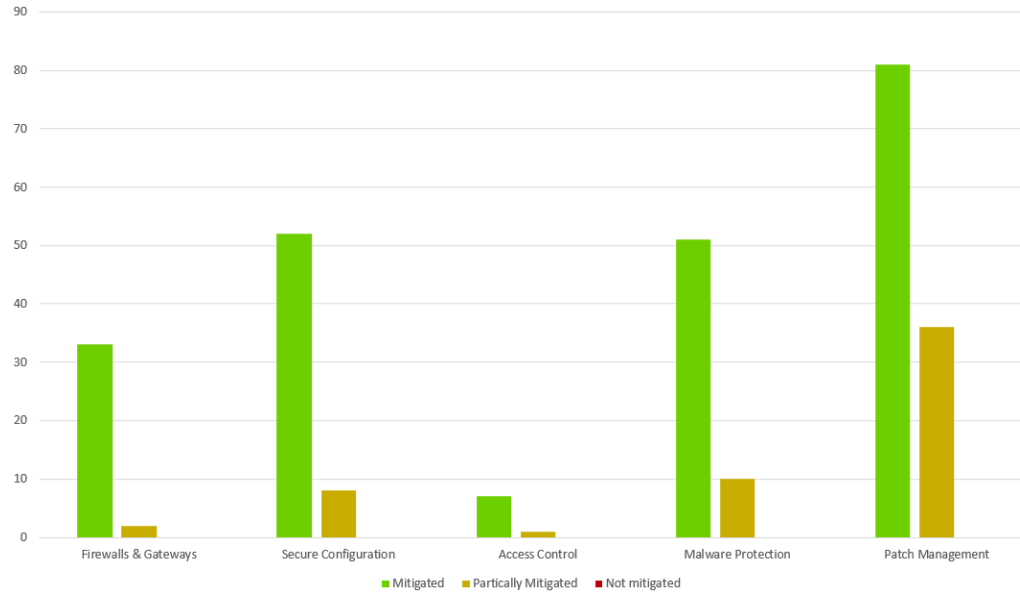
We can also see in Figure 5a that Cyber Essentials controls work very well for the high and very high severity vulnerabilities. Regarding the type of vulnerability, Figure 5b shows that Cyber Essentials security controls performs well across the board, especially on vulnerabilities in the categories of “Denial of Service”, “Gain privilege”, “Execute Code”, and “Cross Site Srcipting”, completely or partially mitigating entirely almost all of them. Regarding the rest of classes, there are good signs coming across from the data, however the small sample of these type of attacks makes it difficult to make definitive conclusions.



(a) Vulnerabilities mitigated by severity



(b) Vulnerabilities mitigated by type



(c) Number of times a security control contributes to mitigate vulnerabilities

Figure 5: Mitigation Assessment by severity and type of vulnerability, and security control.

Patch Management, Malware Protection, and Secure Configuration are most useful

Regarding the effectiveness of each individual security control and its contribution to mitigate vulnerabilities, Figure 5c shows that the control that contributes the most to mitigate or partially-mitigate vulnerabilities is Patch Management, and then Security Configuration, Malware Protection and Firewalls & Gateways. Access control came last as contributing to mitigate or partially-mitigate the vulnerabilities that were applicable to the SMEs studied. This also highlights the importance of security controls like Patch Management. However, a note should be made about their correct implementation. For instance, regarding Patch Management, as we assumed in this paper that it is applied timely and correctly once a patch is available, but evidence from user studies about software update tells us that this may not always happen in practice [21], and that awareness and education mechanisms, together with the collective cyber security approaches described more in detail below, are crucial to maximise its effectiveness. It is also important to stress again that the assessment we carried out considered threats exploiting vulnerabilities remotely with commodity-level tools, so the contribution of security controls to mitigate vulnerabilities coming from other types of threats may be different.

Vulnerability mitigation still relies on 3rd parties

Importantly, 38 of the 40 vulnerabilities judged as *partially mitigated* are as such because they rely of patches from third-party software or hardware vendors, that will be mitigated once a security fix has been released by applying the Patch Management security control of Cyber Essentials. That is, the security involved in using third party software unfortunately relies on the vendor's ability to identify potential areas of risk, as well as to quickly respond to security breaches as they become apparent with the release of patches. The other type of partially mitigated vulnerabilities relied on website blacklisting, combined with avoiding vulnerable web browser software. A secure configuration without such a browser would mitigate this vulnerability, but as in the Web Development (SME 3) case study, it may not always be possible to avoid the use of a specific software piece. In a case as this, website blacklisting, part of the Malware

Protection security control, is the only Cyber Essentials security control against these vulnerabilities.

Only 2 vulnerabilities were immitigable by Cyber Essentials' security controls. These were the cases in which vulnerabilities were due to inherent flaws in a hardware device, or software that cannot be fixed. For these devices that are fundamentally flawed from a cyber-security standpoint, it can be that no level of security tools on top of the network can aid in mitigation - rather the hardware should be replaced to ensure security. It may be possible for a public list of all such devices to be developed to serve as a device-blacklist for SMEs. There indeed exist some collective approaches to improving cyber-security that could be especially useful for SMEs that do not have the resources to keep themselves up to date with the latest security issues, an example of this in the UK is The Cybersecurity Information Sharing Partnership (CiSP) [22]. The partnership aims to benefit all members by providing real-time updates on issues of cyber-security and discovered vulnerabilities, as well as best-practice guides and other cyber-threat information. It would be beneficial for more organisations to belong to cyber-security collectives like this, creating networks of informed individuals working together to tackle cyber-crime. This would be particularly useful to quickly identify potential vulnerabilities and possible patches, which as mentioned above, is critical for the patch management security control to fully mitigate related vulnerabilities. However, vulnerability information shared through these collaborative security systems is provided in highly technical terms and descriptions - which can make them particularly impenetrable to the less technically adept reader. This is further compounded when exploits are described without actually saying the problem, requiring that the reader actually have proprietary knowledge available to them to understand the problem. Ultimately a more accessible, *actionable* form of vulnerability issues needs to be created to allow smaller businesses the chance to implement defences against them before they are attacked.

CONCLUSION

Cyber Essentials seemed to work well in the SMEs studied to mitigate the threats exploiting vulnerabilities remotely with commodity-level tools, appearing to completely mitigate around two thirds of this type of vulnerabilities and partially-mitigating almost a further third, with only few immitigable vulnerabilities. The results may also be partially applicable to other schemes for SMEs in other countries that include/share all or most of Cyber Essentials controls, like the examples stated above of the US NISTIR-7621 "Small Business Information Security: the fundamentals", the Belgian Cyber Security Guide, and the French CGPME/ANSSI "Guide Des Bonnes Practiques De L'Informatique".

It is important to stress that the scope of this study covers only the threats exploiting vulnerabilities remotely with commodity-level tools. In particular, there is an increasingly identified risk from *insider threats* that also requires attention, not least malicious acts, but also from users unknowingly compromising security or falling for social engineering such as phishing. Also, *advanced persistent threats* and other targeted attacks were not considered here. Although one might think that this type of threats target more often bigger organisations than SME, there is evidence to suggest that actually, very targeted attacks coming from those threats now also focus on compromising the digital supply chain of big organisations starting from other, sometimes smaller, organisations (e.g. the infamous example of Stuxnet that reached Iranian power plants [6] indirectly through their supply chain, or the Target and Home Depot breaches [5]).

It is also important to note that the results we obtained are dependent on an almost-perfect adherence to the guidelines to implement Cyber Essentials security controls. While Cyber Essentials is actually one of the very few schemes for SMEs (the only one to the best of our knowledge) that actually includes an assurance framework, i.e., it specifies the way in which adherence to the framework can be assured, a lingering question may still be whether and to what extent an SME certified to have Cyber Essentials adheres to its guidelines, which may have an effect on the effectiveness of its security controls (e.g. see the discussion above about known issues with the implementation of some security controls like patch management). Although recent work has looked at the cost-effectiveness of assurance techniques in revealing the security state of a system in general [18], future work should specifically look at the effectiveness of the assurance

techniques used for SME schemes in assuring adherence to the guidelines and the effect this has in turn in the security controls and their ability to mitigate vulnerabilities.

Another important note to be made is toward the security of business affiliates and service providers. Even if an SME has security controls in place, any use of cloud-services relies on the vendor's security controls for threat mitigation. In other words, cloud-based email, banking and accounting, file sharing, and any other cloud-based or remote services (shown in Table 1 to be of extensive use by SMEs) are only as secure as the service provider makes them. In general, the providers of these services should be encouraged to certify their protection (e.g., through frameworks like ISO27000-series), so that SMEs could make better and informed choices of the cloud services they use.

ACKNOWLEDGMENTS

This cybersecurity project was sponsored by the UK government.

AUTHOR BIOS

Jose M Such is Reader (Associate Professor) in Security and Privacy at King's College London. His research interests are at the intersection of cybersecurity, artificial intelligence, and human–computer interaction, with a strong focus on privacy, AI security, co-owned data, and security controls and assurance techniques in sociotechnical and cyber-physical systems. Contact him at jose.such@kcl.ac.uk.

Pierre Ciholas is a PhD candidate in cyber security at Lancaster University. His research interests include reverse engineering, malware analysis, vulnerability research, programming, and video game hacking. Contact him at p.ciholas@lancaster.ac.uk.

Awais Rashid is Professor of Cyber Security at University of Bristol, UK. His research interests are in security of large-scale connected infrastructures, software security and human (adversarial and non-adversarial) behaviours in these contexts. He leads multiple interdisciplinary research projects on these topics and is a member of the IEEE. Contact him at awais.rashid@bristol.ac.uk.

John Vidler is a Senior Teaching Associate at Lancaster University His research interests are operating systems, networking, and corpus linguistics. His research spans the space between where user interfaces end and continues down through to the electronic and mechanical systems design of computer systems. Contact him at j.vidler@lancaster.ac.uk.

Timothy Seabrook is a PhD candidate in the verification of learning in multi-agent systems, which combines his interests in cyber security, machine learning, formal verification and distributed systems for the purpose of developing certifiable learning systems. Contact him at timothy.seabrook@cs.ox.ac.uk.

REFERENCES

1. United States Census Bureau. Statistics of u.s. businesses (susb) main - latest susb annual data. http://www. census.gov/econ/susb/, 2015.
2. European Commission. Entrepreneurship and small and medium-sized enterprises (smes) - growth.
3. UK Department for Culture, Media and Sport. Cyber security breaches survey, 2017.
4. Ponemon Institute. State of Cybersecurity in Small & Medium-sized Businesses (SMB), 2017.
5. Schmeidler, N. Supply Chain Attacks on Retail – What Happens When Trusted Channels Can't be Trusted? RSAConference, 2017.
6. Kushner, D. The real story of Stuxnet. *IEEE Spectrum*, 50(3), 48–53, 2013.
7. European Union Agency for Network and Information Security (ENISA). Review of Cyber Hygiene Practices, 2016.

8. Cyber Essentials. Cyber essentials scheme - overview. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.
9. Cabinet Office and The Rt Hon Francis Maude MP. Government mandates new cyber security standard for suppliers. https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers, September 2014.
10. HP Aleanna Crane. Hp strengthens uk public sector supply chain with affordable cyber security accreditation for smes. http://www8.hp.com/uk/en/hp-news/press-release.html?id=1771204, September 2014.
11. Kluge, David, and Samuel Sambasivam. "Formal information security standards in German medium enterprises." *Proceedings of the CONISAR: The Conference on Information Systems Applied Research (pp. 30-55)*, 2008.
12. Barlette, Yves, and Vladislav V. Fomin. "Exploring the suitability of IS security management standards for SMEs." *Proceedings of the 41st Annual Hawaii International Conference on System Sciences,* 2008.
13. Dojkovski, S., Lichtenstein, S., & Warren, M. Enabling information security culture: influences and challenges for Australian SMEs. In *ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems*, 2010.
14. Parkin, S., Fielder, A., & Ashby, A. "Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes." *Proceedings of the ACM International Workshop on Managing Insider Security Threats*, 2016.
15. CESG; Cabinet Office; Centre for the Protection of National Infrastructure; Department for Business Innovation & Skills. Common cyber-attacks: Reducing the impact. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf, January 2015.
16. CVE.Mitre.org. Terminology - mitre.org. http://cve.mitre.org/about/terminology.html.
17. Barlett, J. E., Kotrlik, J. W., & Higgins, C. Organizational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, 19(1), 43-50, 2001.
18. FIRST. Common Vulnerability Scoring System. https://www.first.org/cvss/.
19. Such, J. M., Gouglidis, A., Knowles, W., Misra, G., & Rashid, A. Information assurance techniques: Perceived cost effectiveness. *Computers & Security*, *60*, 117-133, 2016.
20. Such, J. M., Vidler, J., Seabrook, T., & Rashid, A. Cyber security controls effectiveness: a qualitative assessment of cyber essentials, Technical Report SCC-2015-02, 2015, Lancaster University. http://eprints.lancs.ac.uk/74598/
21. Vaniea, K., & Rashidi, Y. Tales of software updates: The process of updating software. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (pp. 3215-3226), 2016. ACM.
22. Cyber-security information sharing partnership (CiSP). https://www.ncsc.gov.uk/cisp.