Institution: University of Worcester

Unit of Assessment: 17 Business and Management Studies

Title of case study: Enhancing cyber security for SMEs

Period when the underpinning research was undertaken: 2009-2017

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Richard Henson	Senior Lecturer	1999-present

Period when the claimed impact occurred: 2013-20

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact

A government survey of cyber security threats in 2020 states that almost half of businesses (46%) report having cyber security breaches or attacks in the last 12 months, at an estimated average cost of £3,230 per breach. Collaborative research between academia and business led to the development of an information assurance standard for SMEs and an associated business which subsequently was utilised by government as the basis of a national cyber security standard, Cyber Essentials. This product has been adopted by companies large and small and has mitigated future losses for these companies by enhancing their cyber security systems and protocols.

2. Underpinning research

Henson was the researcher on a project led by the National Computing Centre funded by the Technology Strategy Board to investigate and understand barriers to SMEs engaging with cyber security and to develop an appropriate cyber security standard, risk assessment tool and a scalable and sustainable business model for SMEs (Grant 1).

It was apparent from the start that there were two core challenges:

- Existing Information Assurance Standards (BS7799 and ISO27001) were of limited value to SMEs, given the cost of engaging with these standards.
- Whilst cyber risks were real and increasing (both for businesses themselves and supply chain partners) and businesses were ill-prepared to meet them, SMEs were reluctant to invest even limited time and money in information assurance, seeing this non-investment as an acceptable strategic risk. This was elaborated and expanded in a later paper (see Reference 3).

The standard (available on request), known as IASME (Information Assurance for Small and Medium-sized Enterprises), co-produced by the project team and developed through a pilot with 15 SMEs in the West Midlands, was launched in 2011. It consisted of an assessment and formal certification of the level of maturity of an SME's cyber security that was assurance for itself and its customers. The rationale for this product and the process by which it was developed in described in Reference 1, one of several conference presentations, academic and business, the project team delivered in 2011.

The product was well-received and the decision was taken to establish IASME as a company in 2012. The IASME model assumed that assessors would work with the SME, taking them through the requirements for certification including gap analysis. To make IASME scalable, more assessors would be needed; the university agreed to host the assessor training. However, in spite of the positive feedback from businesses and information assurance experts, the take up of

the project was limited because of the cost of assessment. At this point self-assessment was seen as an unacceptable compromise to the model as there was little incentive for SMEs to be honest in their assessment.

Further research found a solution to this. By building cyber liability insurance into the model, a self-assessment model could be used as clients would only be given insurance cover if they had a base level of cyber security; further, if they went beyond this base level, they would receive a discount (Reference 2). Following this, IASME was relaunched in 2013 at reduced costs with a self-assessment process with insurance included as part of the package.

3. References to the research

1. Henson, R, Dresner D, & Booth, D, (2011), "IASME: Information Security Management Evolution for SMEs", Athens Institute for Education and Research (ATINER) SMEs Conference 2011, 1st-4th August 2011, Athens, Greece.

2. Henson, R & Sutcliffe, D (2013) A Model for Proactively Insuring SMEs in the Supply Chain Against Cyber Risk, Atiner Conference Paper Series No: SME2013-0547. ISSN 2241-2891. https://www.atiner.gr/papers/SME2013-0547.pdf

3. Henson, R and Garfield, J (2016) *What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security?* Athens Journal of Business and Economics, 2 (3). pp. 303-318. https://www.athensjournals.gr/business/2016-2-3-5-Henson.pdf

Grants

1. Henson (Co-Investigator), *Information Assurance for SMEs*, Technology Strategy Board, £75,199 (2009-10).

Output 3 is included in the unit's REF2021 submission and was identified as of 2* standard through the processes set out in the University's REF2021 Code of Practice. Output 1 is available on request.

4. Details of the impact

The research described in section 2 has underpinned the following impacts:

- Creation of a new business, IASME Consortium Limited, which has grown significantly in the assessment period and been recognised nationally for its work
- Development and delivery of a new government-backed Cyber Security product, Cyber Essentials, which has been a key part of the government's Cyber Security Strategy over the assessment period
- Mitigation of future losses through improved risk assessment and management of information for businesses who have engaged with Cyber Essentials
- Contribution to enhanced knowledge and understanding of cyber security risks among businesses and charities

The IASME Consortium Ltd was incorporated in January 2012. It has grown significantly over the last 9 years: by 2020, it worked alongside a network of over 250 Certification Bodies across the UK and Crown Dependencies. Its achievements in the field have been recognised at the National Cyber Awards 2019, where it was named Cyber Business of the Year.

The Department for Business, Innovation and Skills made a call for evidence on a preferred standard for cyber security in 2013. The findings of this call (Source A) and the government response (Source B) were published in November 2013. The report highlighted the strengths of IASME as a product and the government response identified IASME as one of a small number of tenable models. The outcome of the call was to develop a new preferred standard working with

IASME and the Information Security Forum; the value of IASME in this process was highlighted because of the simplicity of the model and its relevance to small businesses thus aligning with government's 2011 Cyber Security Strategy which highlighted the specific need to make sure that SMEs are aware of cyber security risks and that they benefit explicitly from policy and practice.

The new standard, Cyber Essentials, was launched in 2014 as a product of collaboration between government, IASME and ISF (Source C). The product, backed by the CBI, the Federation of Small Businesses and a number of insurance organisations, provided a simple, low-cost set of basic technical controls to help organisations, large and small, to protect themselves against common online security threats. As such, it owed a great deal to the original IASME model.

From October 2014, Government required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme. Subsequently, commitment was made by a number of large employers (e.g. Airbus, Barclays, BT, Vodafone) to encourage their suppliers to engage with Cyber Essentials (Source D).

A 2016 Government Cyber Health Check and Cyber Security Breaches Survey, highlighted the value of the scheme:

"Last year, the average cost of breaches to large businesses that had them was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experienced a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme" (Source E).

In October 2019, it was announced the IASME Consortium had won the 5-year contract to be the National Cyber Security Centre's Cyber Essentials Partner from April 2020 (Source F). 60,000 certificates have been issued since its initial implementation and currently around 1500 new businesses are being certified every month.

Surveys undertaken for government on cyber security breaches in 2016 and 2020 (Sources G and H) have demonstrated the growth, from 48% to 51%, in businesses' knowledge and understanding of the five technical controls embedded in Cyber Essentials even where those companies do not necessarily have accreditation. This highlights the effectiveness of Cyber Essentials in raising awareness of cyber security risks and potential mitigations.

5. Sources to corroborate the impact

A. Department for Business, Innovation and Skills (November 2013), *UK Cyber Security Standards: Research Report*
B. Department for Business, Innovation and Skills (November 2013), *Call for evidence on a preferred standard for cyber security: government response*.
C. Cyber Essentials Scheme: overview - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
D. Matt Hancock's cyber security speech at the Institute of Directors conference (March 2017) - https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference
E. National Cyber Security Strategy 2016-21
F. Press release announcing the IASME Consortium is the National Cyber Security Centre's Cyber Essentials Partner: https://www.ncsc.gov.uk/blog-post/announcing-iasme-consortium-as-our-new-cyber-essentials-partner
G. Cyber Security Breaches Survey 2016
H. Cyber Security Breaches Survey 2020