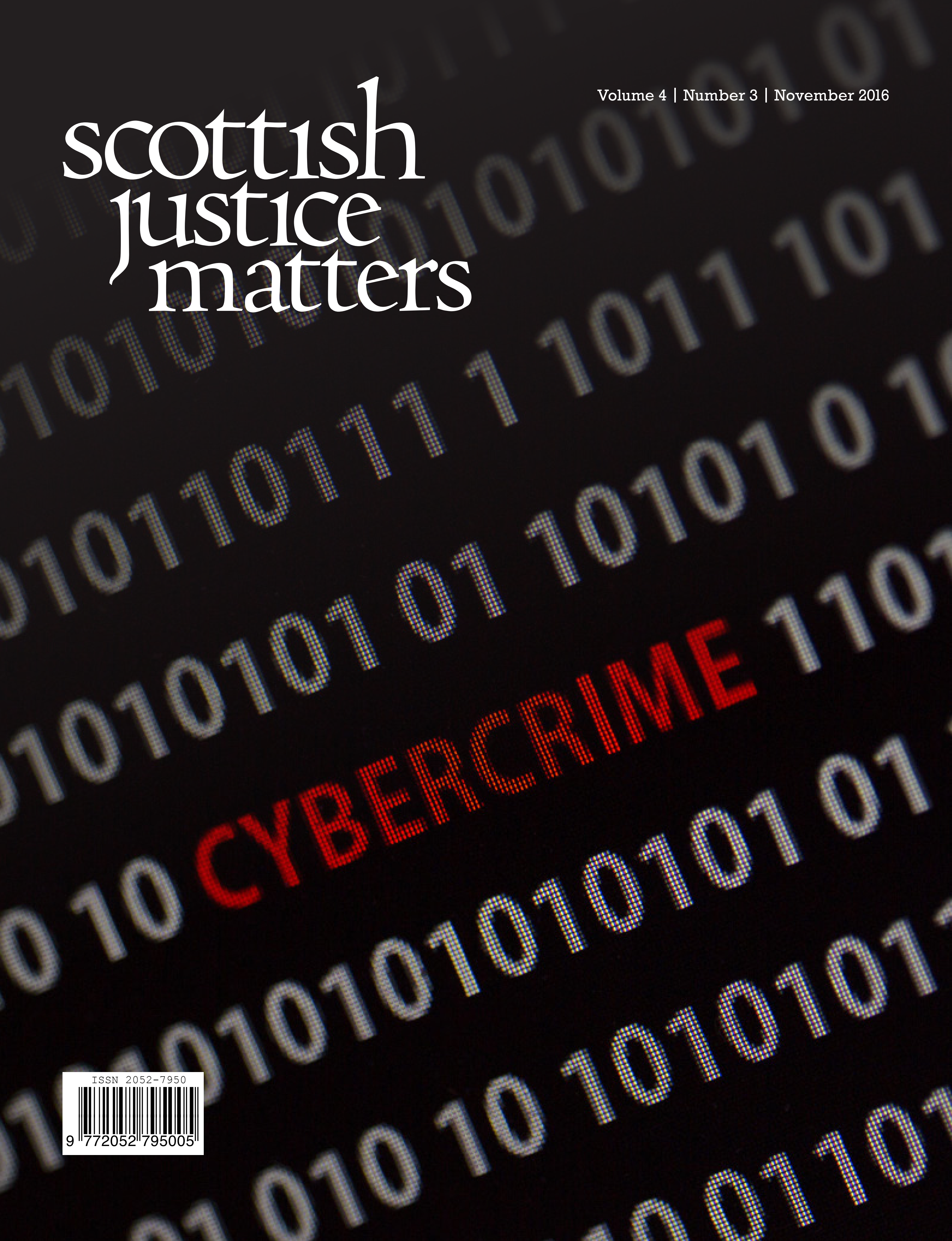
Volume 4 | Number 3 | November 2016

# scottish justice matters



ISSN 2052-7950
9 772052 795005

# CYBERSECURITY AND SMALL BUSINESSES

**Mandy Haeburn-Little** on the work of the Scottish Business Resilience Centre

**IT USED TO BE** that the fastest way to kill off any conversation was to say you were an accountant, but now the fastest ways to get that glazed expression is to be a cyber-security consultant trying to persuade a (small) business that cybercrime represents a real problem.

Given that we are seeing a steep rise in the number of cyber attacks (ransomware is already breaching 1 in 3 companies) (Kujawa 2016) and that Scotland ranks as the lowest area of the UK in actively adopting cyber preventative measures (Taylor 2015), why is the glazed expression so common?  What is going on?  Or rather, what is not going on and what should be done to turn that round? How can we help members of the business community embrace their responsibility for cyber protection and give them a degree of confidence that they are doing the right thing?

Part of the response has been the creation of the Scottish Business Resilience Centre, a membership organisation for Small to Medium Enterprises (SMEs) offering advice on various aspects of doing business in the face of criminal activity. The SBRC's cyber program seeks to educate and advise members on the threat of cybercrime and possible responses.

There can be no doubt that crime has moved online when in October 2016, for the first time, reported Internet crime overtook traditional physical crime (Office of National Statistics, 2015). Despite such statistics being readily available, small businesses often exhibit a head-in-the-sand attitude and there is a lack of coherent approach within the private sector to the potential scale of the problem.

There may be a number of reasons for the threat being taken lightly. One may be the image of the hackers themselves. It is hard to think back to when the threat of hackers in hoodies crept around the corner of our consciousness. A hacker became a 'sexy' thing to be, an unknown, someone with skills that ordinary mortals do not understand, anti-heroes who have superpowers without boundaries. The media have struggled with the morality of hacking: how can hacking be both a good thing and a bad thing? Those seeking to limit the influence of world superpowers, global threat actors or malign international agencies are sometimes portrayed as whistle-blowers and hacktivists, but when the resulting reality behind the imagery is of an (archetypical) teenage loner with learning difficulties, a different and complex picture emerges.

It could be that small businesses look at such imagery and wonder "What interest would they have in me?" Unfortunately, this image of the hacker is out-dated. Today's organised cybercrimes are often not targeted and are not performed by humans: they are automated systems that have no concept of who or what their target might be. They are simply programs operated by organised gangs of criminals automatically scanning for vulnerabilities in security. Several cybersecurity companies have now stepped back from using the term 'hacker' because of the mistaken image promoted.

A second reason for the threat being taken lightly might be the attitude that as it is a technological problem, then technology will solve it. The nature of cybersecurity however is such that it is not solely a technological problem, it is a human behaviour problem. Appropriate cybersecurity behaviour requires both knowledge and motivation from an entire organisation. One weak password or one incidence of risky behaviour towards malware ("It's only one hooky movie download, it can't hurt") can completely compromise a whole organisation.

This brings us to the third possibility: lack of skills, knowledge and motivation. If you do not know the consequences of a cyber attack, you are unlikely to be bothered about it. The skills agenda is so important. I have recently spoken at a number of events aimed at persuading girls of school age to aim for careers in the digital area, whether it be creating a new product, changing the future face of medicine, controlling cars of the future or being an trailblazer in design and brand evolution. At one of these events, I was faced with an audience of girls really keen to be involved. Behind them sat the teachers from their different schools. My message to the girls was to challenge their teachers and to ask for more, to be taught more, to be challenged in what they wanted to learn. Meanwhile behind the girls, the teachers looked less than enthusiastic simply because they have not been equipped with the digital skills.

Scotland has at times been less than nimble to provide the leadership needed on digital and cyber skills, however in my view it remains a model for future success. The Scottish Government launched the Cyber Resilience Strategy for Scotland in November 2015. Under this banner there exists a leadership group to deliver the strategy focusing on five 'pillars' (or themes): Communications, Public Service, Research, Business Enablement and Skills. This is a solid foundation that needs to progress. The UK's first National Cyber Security Centre was launched in October 2016 and we look forward to seeing the substantial offering and support beyond its vision.

In the interim however, business will not wait. The needs of consumers and business and citizens will continue to grow as we move to digitalised and automated services, where everything from accessing your health record to agreeing a company loan can and will be done without human interaction. So what is the solution?

One interesting approach to the problem has been adopted by the SBRC. In a small-scale cross-sectoral project (supported by law-enforcement and the commercial sector) students, drawn from Abertay University's BSc Ethical Hacking course, have been offered internships. Their role can be summarised as "educate, assess and advise." They provide demonstrations of the kind of capabilities that hackers possess in public/business facing events.  As well as this, they visit SMEs, assessing their basic cybersecurity (using ASSAM, the Abertay SME Security Assessment Methodology) and providing clear reports on shortcomings. This model has now being adopted further afield in the London Digital Security Centre.

Over the four years the SBRC has been working in partnership devising new affordable services for business, all of those students, on graduating, have relocated down South to work. Why? The perception is still that you have to travel to get the big roles. Scotland may provide the best possible nursery, but the opportunity still lies elsewhere. Although the SBRC/ASSAM approach has been successful, it is limited in scale and a more comprehensive approach is needed.

**A twofold solution is proposed.**

**1.** A 'Cyber Hub for Scotland' should be created working across sectors with preferred suppliers: a single point of contact for companies facing cybersecurity problems. This would support, at the lower level, the business demand for the growing and excellent cyber business network the SBRC has. At a higher level it would quickly provide trusted partners for the most complex of situations; a 'Tier 1' of gold suppliers of more sophisticated ability. Underpinning all of this would be a triage system for cybersecurity incidents, available to businesses and citizens, operating 24 hours a day where advisors (drawn from apprentices, interns and undergraduate ethical hackers) and smaller technical companies are available on demand to help direct and ease the burden of lower level enquiries currently shouldered by law enforcement.

From this model, apprenticeships to the larger cybersecurity companies can grow and develop. The academic cybersecurity community in Scotland can offer outstanding state of the art skills programmes and communities of knowledge. We can research and develop new and even more complex responses and solutions. Police, local, national and international Government would have ready access to all the analytics that underpin this. Perhaps most importantly, Scotland could learn from some of the outstanding public/private/academic partnerships that we have seen flourish elsewhere from, for example, Israel, Estonia and Norway.

**2.** We must work much harder on the business community's understanding of cybersecurity, creating a commonality of language. For example, we could make cybersecurity proficiency a condition for the bank loans that are given for growth and for public start-up funds that are accessed. Does your business have the necessary basic understanding of what you need to do to keep your business, your data and that of your customers safe? The insurance industry also has a role to play here by offering simple cyber insurance products only to those firms that can demonstrate cybersecurity competence.

Scotland is defined by its strong history of innovation. Universities are producing some genuinely jaw dropping talent whether it be in digital forensics, cryptography, STEM research or, closer to home, a quite unique band of ethical hacking experts from Abertay. Academia across Scotland is leading the way. We have a growing digital and cyber community of small and growth businesses and are actively seeking to attract more of the same. Business must now choose to act on the threat.

**Mandy Haeburn-Little** is director of the Scottish Business Resilience Centre.

Kujawa A (Malwarebytes)(2016) *Ransomware doesn't mean game over.* https://blog.malwarebytes.com/101/2016/11/ransomware-doesnt-mean-game-over/

Office of National Statistics (2015) *Crime in England and Wales: Year ending June 2015*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/2015-10-15/pdf

Taylor P  (KPMG/CyberStreetwise) (2015) *Small Business Reputation and Cyber Risk* https://assets.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf