Editorial

Oredola A. Soluade

Hagan School of Business,
Iona College,
New Rochelle, 10801 New York, USA
Email: osoluade@iona.edu

1 Introduction

In the last few years, mobile, social, big data and analytics have fuelled tremendous shifts in how companies work, what customers expect and how systems should be connecting. There has been a plethora of security breaches in the past few years; including the release of secret US Government papers by Snowden, the release of the Panama papers, and news about terrorist activities and their associated intelligence-gathering, in Paris and Brussels. There has been a dramatic increase in the use of cloud services to run global companies; and this makes them very vulnerable to cyber security breaches. Secure and resilient models will have to be developed to mitigate operational exposures and protect data intrusion.

2 Subject coverage

There is a broad range of topics covered in this special issue on cybersecurity. Issues relating to global oil price fluctuations and its impact on security, to the impact that quality assurance has on the maintenance of security in a quality assurance environment, to protection and preservation of networks from security breaches and cyber-attacks, to using trajectory anonymisation using multidimensional index structures, and to assessing the skills required for support of effective organisational risk management

3 Special issue

In their article titled ‘The mimetic virus: a vector for cyberterrorism’, Ayres et al. argue that cyberterrorism has the same aims and goals but the act is done exclusively within cyberspace where the computer is both weapon and target. Unlike conventional terrorism, cyberterrorism is not analogue but digital and any potential attack could have global consequences. Current thinking is that critical network infrastructure is the main target of focus for cyberterrorism but with so many people online on a national or even global scale, public structures could prove to be an easier, more tempting target. The article addresses how the cyberterrorist could use the public as target of a real or fake attack by using a mimetic virus as the weapon.

Ojumu and Opara analysed the USA as a net importer of oil. The paper uses a balance of goods and services (BGS) model to trace the effect of oil price variation on selected macroeconomic variables in the USA, and the cybersecurity implications of oil price variation controls the balance of payment (BP) through money supply and exchange rates.

Soluade identifies application quality assurance as a critical phase of application development; which is the last stage at which a product is subjected to a series of tests before it is generally available to the customer. He highlights the criticality of ensuring the integrity of the product-certification process. He identifies a series of possible breaches that can occur and attempts to identify, design, and develop a strategic plan that will minimise the possibility of security leaks in the development process.

Almasrahi et al. argue that trajectory datasets are increasingly available due to the technological advances in location-tracking devices such as GPS, wireless technologies, and hand-held device. In this issue, privacy issues of publishing trajectory datasets using trajectory k-anonymity, which anonymises each trajectory with $k - 1$ other trajectories are analysed. Since the original R-tree may provide more than desired level of privacy, a novel algorithm has been proposed, which can ensure that the level of privacy is no more than required.

According to Opara and Mahfouz, security breaches of all kinds are growing in complexity, sophistication, and impact. Security professionals have invested billions of dollars into conventional defences. Yet, attackers are compromising networks at an alarming rate. Regardless of what tools an organisation deployed, attackers are bypassing these with ease. This issue includes a study that analyses the awareness among security practitioners so that that they can be adequately prepared to defend their enterprise system. With new opportunities in mobile, social and other technologies one will have to connect systems and applications in new ways, including across hybrid cloud environments. Open technologies give you the flexibility to deploy your services across a wider range of platforms, allowing one to more easily connect your existing systems with new systems that expand your reach to customers. However, these connectivities are fraught with danger of cyber threats – ranging from session hijacking attacks, Java attacks, operating system attacks, and zero-day attacks.

In her article, Munsch discusses the skills needed for an effective consulting engagement and how this is in support of effective organisational risk management. The client's underlying concerns about exposure, vulnerability and control are explored. Self-awareness, examining resistance and in particular, authenticity in consulting engagements are also discussed in terms of their overall importance to effective mitigation of security breaches.

4 Invitation to contribute

The editorial team of the *International Journal of Business Continuity and Risk Management* invites both professionals and academics to contribute their work to the journal in order to continue this important discussion and to advance our knowledge in this critical area of study. Authors can submit contributions investigating the impact of cyber terrorism on the integrity of global networks. All papers are refereed through a double blind review process.