Issue 1 | April 2018

Commonwealth Auditors General Group e-newsletter

Introduction by Sir Amyas Morse, Guest Editor

I would like to begin by saying how pleased I am to edit the first e-newsletter of our Commonwealth Auditors General Group. On behalf of myself and my fellow editors, the Auditors General of Australia, Jamaica, Fiji and Tanzania, we would like to thank the Supreme Audit Institutions (SAIs) of Australia, Malta and my own team in the UK for producing the articles below. We chose cyber security as the theme for this newsletter as it is the next part of the conversation on 'leveraging technology in public audit' which was started in New Delhi at the XXIII conference. We discussed how the governments we audit are looking more and more towards information technology to manage resources and deliver complex public services. We also discussed how many SAIs are investing in the opportunity to use new audit approaches such as data analytics to deliver more cost-effective audits.

Cyber security is in many ways the other side of this coin. The recent global attacks have been a wake up call for many Governments who, for good reasons, are seeking to use technology to innovate public service delivery. Our performance audits often recommend efficiency gains through automation, or improved decision making through using better information derived from the analysis of vast sets of data. However, I believe that when we encourage innovation, we should ensure this does not compromise security. I am sure you would agree this can be a difficult balance for governments to achieve.

One of the main purposes of this e-newsletter is to share experiences and establish a dialogue based on the discussions we started in New Delhi. As the articles from Australia, Malta and the UK demonstrate, SAIs cannot lose sight of the risk to the public if the information systems which governments are increasingly reliant upon are vulnerable to attack. Each article sets out how the three SAIs have developed an audit programme in response to the risks specific to their national context. What is also clear from the articles, is that as we access and use more data in our audits, our SAIs also need to invest in keeping our houses in order. This again has implications for how we are funded and resourced.

The ANAO article introduces the work of the Australian Signals Directorate (ASD) in developing prioritized mitigation strategies to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies for targeted cyber intrusions and ransomware is known as the Essential Eight Model – a useful tool to help organisations save time and money. The model has been used by the ANAO in recent fieldwork. Malta's NAO has conducted a number of IT audits in various government departments. Their horizontal audit of ten government entities compares the level of adoption of cyber security controls across auditee sites and provides us with some of the key findings.

In the UK's example we have a series of lessons to be learned from the Wannacry incident which not only affected the UK government but can be applied to organisations around the globe. We have also found that many public sector audit committees have been struggling to engage with cyber issues, so the NAO has published guidance specifically tailored to their needs which complements government advice by setting out high-level questions and issues for audit committees to consider.

At the XXIII Conference, Auditors General agreed that it would be beneficial for our group to continue working with key Commonwealth organisations which might include engagement with the Commonwealth Association of Public Accounts Committee (CAPAC) and other parliamentary groups. I am therefore grateful to the Commonwealth Parliamentary Association UK for their contribution to this e-newsletter. The CPA have designed an e-Handbook for parliamentarians on cybersecurity & cybercrime which combines good practice case studies, advice, ideas and innovation to assist international parliamentarians in legislating, scrutinising and advocating policies relating to cybersecurity and cybercrime.

The discussions in New Delhi affirmed the value we place on our Group. Our shared history, Parliamentary system, and language are some of the factors which make the Commonwealth Auditors General Group unique In addition to producing e-newsletters such as this one, we plan to schedule a meeting of Commonwealth Auditors General at INCOSAI XXIII in Russia (September 2019), and of course there is our next meeting in Fiji, 2020. This provides us with an opportunity to discuss matters of mutual professional interest and concern, and to share experiences with the aim of improving the way we serve the 2.5 billion citizens from the fifty three member countries of the Commonwealth.

I hope you find the e-newsletter as thought provoking as I did, and I look forward to reading any thoughts you may wish to share with your fellow Auditors General in response to the articles. Going forward, if you would like your SAI to be involved in producing the next e-newsletter, or if you have any thoughts on future technical content which you would like to propose, please do contact my team at: international@nao.gsi.gov.uk.

Amyas

Contents

3
Australian Government cyber security environment

5
Horizontal Audit on Cyber Security across Government Entities carried out by Malta's National Audit Office in 2017

7
The Work of the UK National Audit Office on Cyber Security

9
News from the Commonwealth Parliamentary Association UK (CPA UK)

9
Timeline of key milestones

Australian Government cyber security environment

In 2010 the Australian Signals Directorate (ASD), Australia's national authority for signals intelligence and ICT security, identified four strategies (application whitelisting; application patching; operating system patching; and access provisions for privileged user accounts) that an entity could implement to prevent 85 per cent of targeted cyber intrusions. In 2013 the implementation of these strategies was mandated for all Commonwealth government entities. Effective implementation of the mandated strategies assists entities to control their ICT systems, and provides a higher level of assurance that systems will support business services.

Since 2013 the Australian National Audit Office (ANAO) has conducted three audits that assessed eleven entities' compliance with the mandated strategies, and their effectiveness in the management of cyber risks.

ANAO cyber security audit approach

The ANAO cyber security audits have drawn on specialist IT audit skills and experience to examine controls at four security layers: gateway; network; application; and desktop.

The audit approach included:

- developing and running Computer Assisted Audit Techniques to interrogate and report on installed application and operating system versions and security patch levels
- examining configuration of controls at the server and desktop level
- reviewing the effectiveness of ICT governance frameworks, including policies, procedures and staff training.

The ANAO's summary findings for each auditee are reported in the form of a graphical matrix. This matrix indicates entities' overall compliance with the mandated strategies and the underpinning IT general controls.

What we have learned

Achieving cyber resilience

As long as cyber security is seen as primarily an IT problem rather than an impact to business services, entities are unlikely to achieve the desired level of cyber resilience. Cyber resilient entities recognise that cyber security is a business risk and manage accordingly.

Compliance vs cyber security culture

The mandating of a minimum set of controls has led to a discussion in the Australian government IT security arena about whether having a compliance approach, directed at implementing controls with the primary objective of achieving compliance, actually hampers an entity's achievement of cyber resilience. In these discussions it has been suggested that embedding the right culture is more important for achieving the desired outcome. The ANAO's audit observation is that compliance is an indicator of cyber security culture, where an entity has embraced the need for cyber resilience, one of the markers is that it has effectively implemented the mandated controls.

Graphical presentation

The ANAO's cyber security audits have garnered a high level of interest from Parliament, Australian Government entities, industry and the media. The graphic matrix is a key communication tool as it includes the ability to compare where entities are positioned in terms of their cyber security resilience (see **Figure 1** below). An entity's position on the matrix indicates its overall ICT security posture, in essence how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and unauthorised disclosures, and how well it is positioned to address threats.

Way forward

In June 2017 ASD released the Essential Eight Model to assist entities to assess the level of implementation of the (now) essential eight strategies. In November 2017 the ANAO commenced audit fieldwork in assessing three Australian Government entities against the Essential Eight Maturity Model.

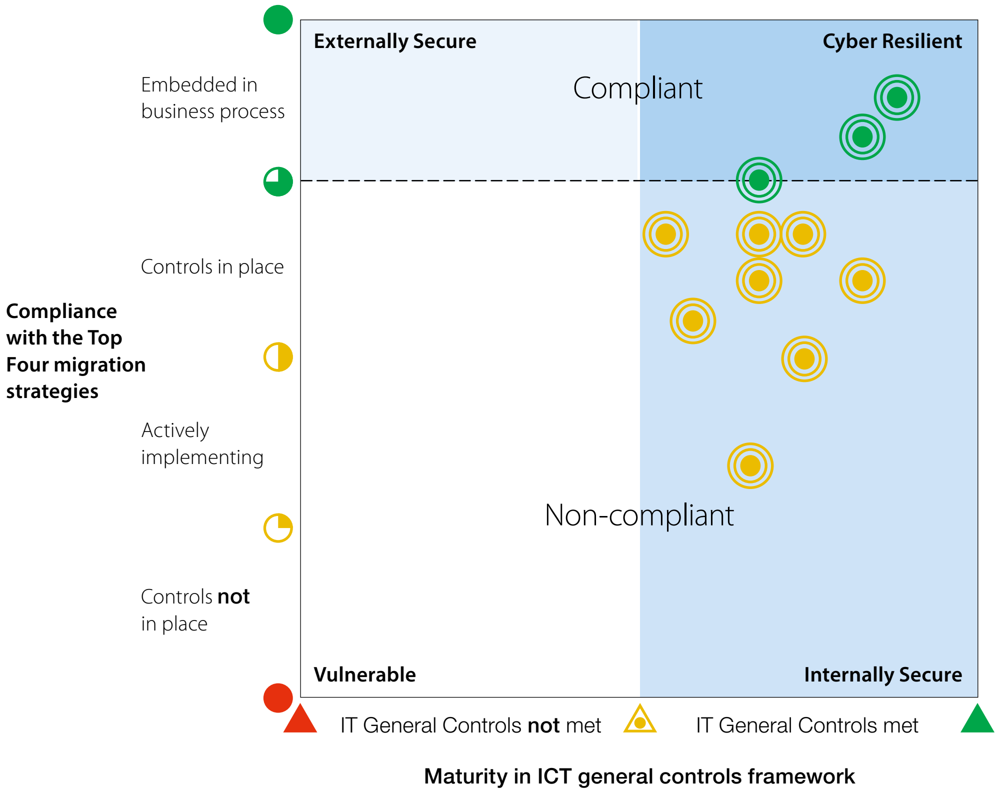
For more information on the ANAO's cybersecurity work, contact:

Peta Martyn

Executive Director – Professional Services and Relationships Group: external.relations@anao.gov.au

Figure 1

ICT security posture for eleven Australian Government entities between 2013 to 2017



Source: Australian National Audit Office (ANAO)

Horizontal Audit on Cyber Security across Government Entities carried out by Malta's National Audit Office in 2017

Over the past five years Malta's National Audit Office (NAO) conducted a number of IT audits in various Government Departments and Entities. Certain findings were common across the different IT audits, in particular, inadequate controls protecting Government Departments and Entities' exposure to external vulnerabilities and intrusions, internal breaches and disclosures. Considering the risks involved, the extent to which entities were adequately positioned to address such threats was often a cause for concern.

Within this context, the NAO embarked on a horizontal audit to compare the level of adoption of selected Cyber Security controls across selected auditee sites. The horizontal audit was conducted across ten different Government Entities.

Key findings

The following is a list of key findings noted by the NAO during the execution of the above mentioned audit at the 10 selected Government Entities (referred to hereunder as "Entities"):

- Some of the smaller Entities opted to fully outsource their IT services without having in-house IT resources to manage these outsourced services and the entity's IT requirements and IT risks.
- Only one of the ten Entities had a Data Retention and Storage Policy and in this instance, the policy was under review and not being adopted. Similarly, only one of the Entities had an Information Classification Policy. Three of the Entities did not have any Internet and e-mail usage policies.
- Most of the Entities were not regulating the use of portable storage media devices and limiting or discouraging the connection of such devices to the Entity's network except where there was a valid business case for their use.
- Two of the Entities did not implement any password complexity rules, neither on their PCs nor on their software, whilst another four Entities opted to implement password complexity rules when logging onto their PC's and when accessing e-mails, but not in order to access their software applications.

Given that the results stemming from this horizontal audit tended to be similar to the ones emanating from the full IT audits that the NAO had concluded in the past, especially those conducted in Government Entities, the NAO considered these audit findings as highly indicative of the scenario and thus rated each criteria examined in this audit, for each of the 10 audited sites, using a Maturity Model so as to provide a general picture indicating where Government Entities are positioned in terms of Cyber Security (see Figure 2 on page 6).

The NAO was pleased to note that most of the feedback given to the Entities was duly taken on board and some of the auditees even embarked on improving their situation while the audit was still underway. The Entities submitted timelines (included in the report) for the implementation of the recommendations made by the NAO. The audit was concluded with an exit meeting attended by representatives of all the audited entities where auditees were given an overview of the overall audit and related outcomes. This Office intends to follow up and report on the progress made in the implementation of its recommendations.

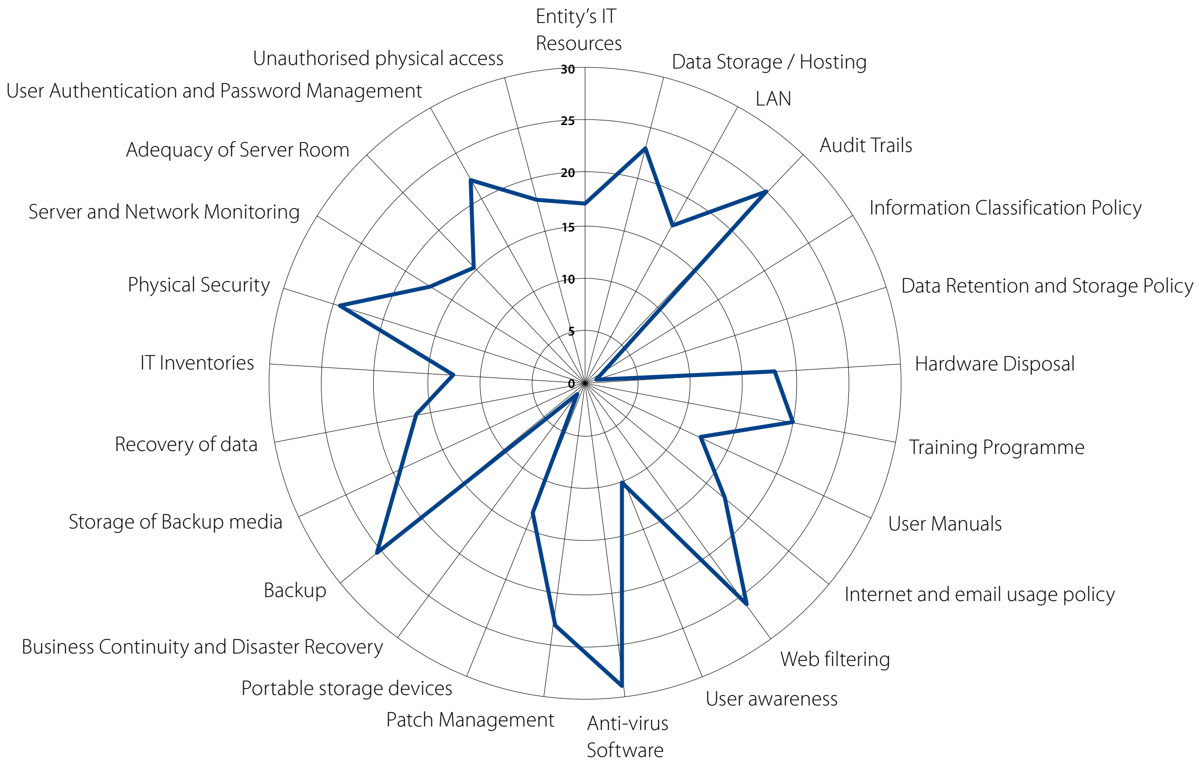
For more information contact:

Simon Camilleri

Manager IT Audit and Support Unit, National Audit Office of Malta: simon.a.camilleri@gov.mt

Figure 2

Cyber Security across Government entities



The resulting figures plotted in the figure above, were the summation of these ratings, across all audited Entities for each audited criteria. Each criteria was rated for every Entity using a grading scheme whereby:

0 – Controls not in place; 1 – Controls partially in place; 2 – Controls partially implemented; 3 – Controls fully implemented; 4 – Controls reviewed and improved periodically as part of the Entity's normal business process.

Source: Malta National Audit Office

The Work of the UK National Audit Office on Cyber Security

Why it is important

Addressing the challenges of cyber security is a clear priority for the UK Government. In the 2010 National Security Strategy, cyber was classified as a "Tier 1 threat", meaning that the Government saw it as an equally high threat as a conventional military attack or a natural disaster. And as the UK's economy and public services become increasingly digital, it is vital to ensure that online activity is secure and trusted.

In 2011, the Government published its first national cyber security strategy. With a budget of £860m, it attempted to increase the capability of central government to deal with cyber security challenges and then work in partnership with others to make the online activities of the private sector and individual citizens safer and more secure. But, by the end of the strategy period, the Government recognised that, although it had made some progress, it had not achieved the scale and pace of change required to stay ahead of what had become a fast-moving threat.

So, in its second national cyber security strategy in 2016, the Government allocated a further £1.9bn over the next five years and re-cast its approach. The new strategy is to be implemented through three areas of activity, known as "Defend", "Deter" and "Develop". Key aspects of this strategy were to establish and embed a new National Cyber Security Centre, to more actively defend UK networks and to improve the depth and breadth of cyber skills available to UK public and private sectors.

What we are doing about it

The UK National Audit Office is responding to the challenge of auditing cyber security expenditure in three ways.

Firstly, we are auditing direct cyber security expenditure by assessing the effectiveness of the National Cyber Security Programme and other central government activities designed to protect data. Our reports on the National Cyber Security Programme and Protecting Information across Government are examples of this work. Both of them set out the considerable challenges involved in protecting information while re-designing public services and introducing the technology necessary to support them.

Secondly, we are auditing cyber elements of other programmes and government's response to specific cyber security incidents. Increasingly, we see cyber security considerations featuring in a wide range of projects and programmes, from digital transport schemes to smart energy meters and secure online financial transactions. And, as we noted in our report on Online Fraud, the internet is changing the nature of crime and law enforcement responses are struggling to keep up (see Figure 3 on page 8). As more and more public services are delivered online and internet connectivity is increasingly a feature of everything from military equipment to medical technology, consideration of the cyber elements of these programmes is likely to become a bigger part of our work. A good example of this is the WannaCry incident, which affected many National Health Service institutions along with other organisations across the world. In October 2017, we wrote a report setting out some of the shortcomings in the Government's response to help it improve for the next breach or incident.

Thirdly, we are equipping and upskilling our staff so that they can in turn help our client bodies think about the cyber issues they face. We have added new activities to our long-standing training of IT and systems auditors to engage a broader range of staff. During our annual training and development week, we have arranged for government and industry representatives – including the head of the UK's new National Cyber Security Centre – to come and speak to staff so that they have the latest picture of developments. We also share insights with colleagues who have expressed an interest in the area through blogs, article recommendations and guidance. A popular resource is our recent publication of guidance for audit and risk committees, which has been particularly well received by small and medium sized client bodies. It provides a checklist of questions covering issues we know our client bodies are concerned about, including:

- The overall approach to cyber security and information risk management;
- The capability needed to manage cyber security;
- Specific aspects such as information risk management, network security, user education, incident management, malware protection, monitoring, and home and mobile working; and
- Related areas, such as using cloud services and developing new services or technology

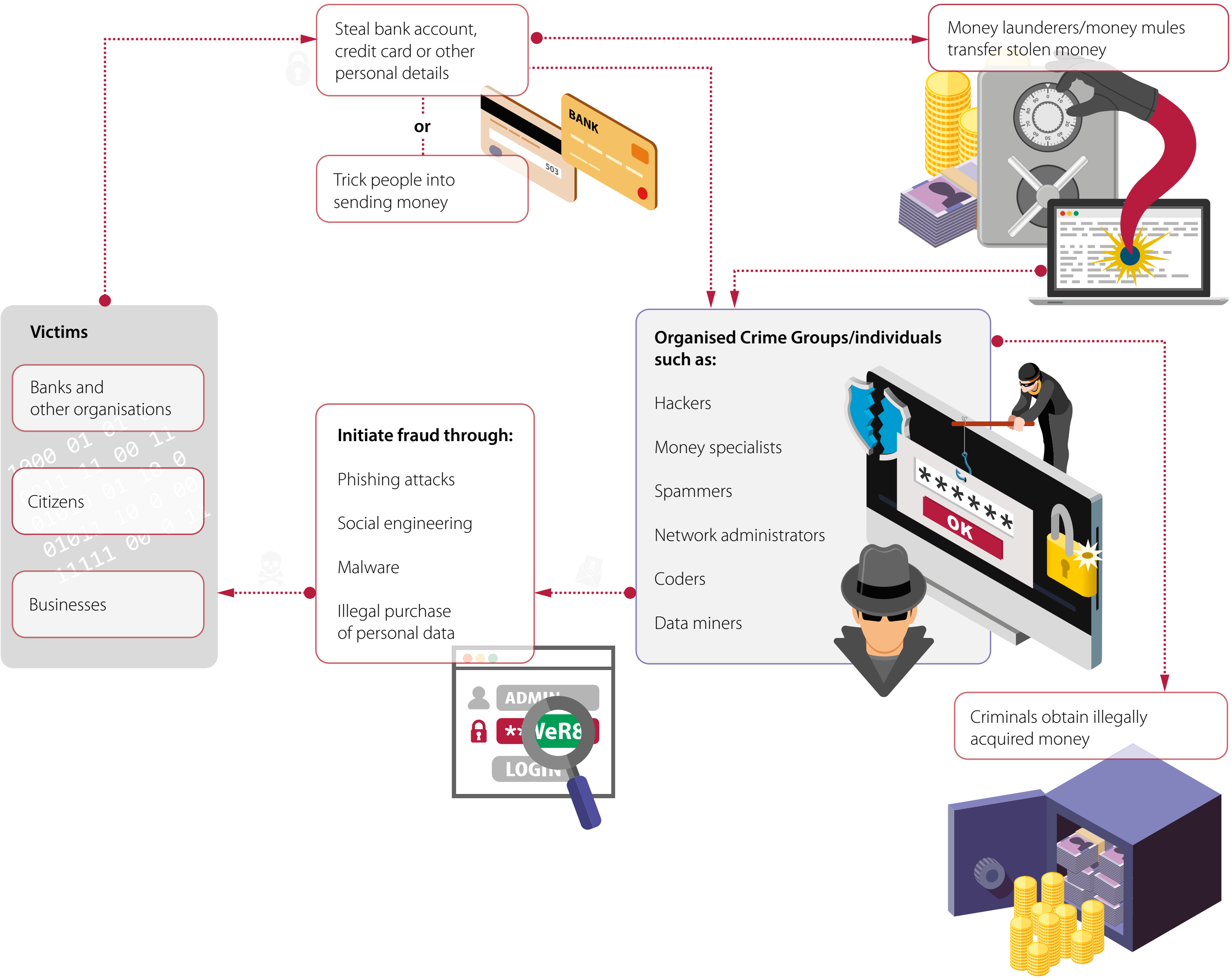
This is a fast-moving area and we continue to try and learn alongside our client bodies in order to keep up with technical and policy developments. We know from discussions with many of those clients that they lack the experience and skills to deal with new developments in technology and the more we can do to spread good practice and awareness, the better we can help equip them to deal with those developments. Alongside all of this work, of course we need to keep our own house in order, since we hold sensitive data from our clients as well as data relating to our own management and operations. So we have dedicated considerable efforts into improving our own information security practices and improving NAO staff awareness. But we recognise that this is an ongoing process and that, like our clients, we will have to remain alert and agile in order to keep our information safe.

Tom McDonald is the Director responsible for the UK National Audit Office's work on cyber security. For more information contact tom.mcdonald@nao.gsi.gov.uk

Figure 3

An example of how criminals commit online fraud

Criminals often have sophisticated business operations to commit online fraud



Steal bank account, credit card or other personal details

or

Trick people into sending money

Money launderers/money mules transfer stolen money

Victims

Banks and other organisations

Citizens

Businesses

Initiate fraud through:

Phishing attacks

Social engineering

Malware

Illegal purchase of personal data

Organised Crime Groups/individuals such as:

Hackers

Money specialists

Spammers

Network administrators

Coders

Data miners

Criminals obtain illegally acquired money

Source: National Audit Office

News from the Commonwealth Parliamentary Association UK (CPA UK)

On Wednesday 22 March 2017 a terrorist attack was committed in Westminster, the heart of UK parliamentary democracy. This tragic event, like so many terrorist attacks across the globe, breed online and are supported through funds from cybercriminality. That is why it is becoming increasingly vital to find international solutions for these international problems that grow and spread across cyberspace and the Commonwealth network is one way to provide a collective approach to tackle this challenge at both a state and corporation level.

The week following the attack, the Commonwealth Parliamentary Association UK (CPA UK) hosted an International Parliamentary Conference on National Security and Cybersecurity. During the conference, the Chair of the UK's Joint Committee on National Security Strategy, the Rt Hon. Dame Margaret Beckett MP addressed the commonwealth audience and stressed that "parliamentarians must utilise their legislative, budgetary and oversight powers to influence the shape and content of national security and cybersecurity strategies…"

This event was the culmination of a year-long Cybersecurity and Cybercrime Project funded by the FCO and in partnership with CPA UK, the Organisation of American States and the Commonwealth Secretariat. The Project comprised of a series of three regional parliamentary workshops held in Africa, Asia-Pacific and the Caribbean to build the capacity of parliamentarians, ministers and senior civil servants. By focusing on legislation, scrutiny and implementation, the project aimed to form a resilient cyberspace and strengthen international and multi-stakeholder cooperation.

As part of this project, CPA UK, developed an International Parliamentarians' e-handbook on cybersecurity and cybercrime to provide a global audience of parliamentarians with a resource in tackling this modern day crime.

A collective approach must therefore be taken at both a state and corporation level. However we also need to take responsibility for our own cybersecurity and encourage others to do their part.

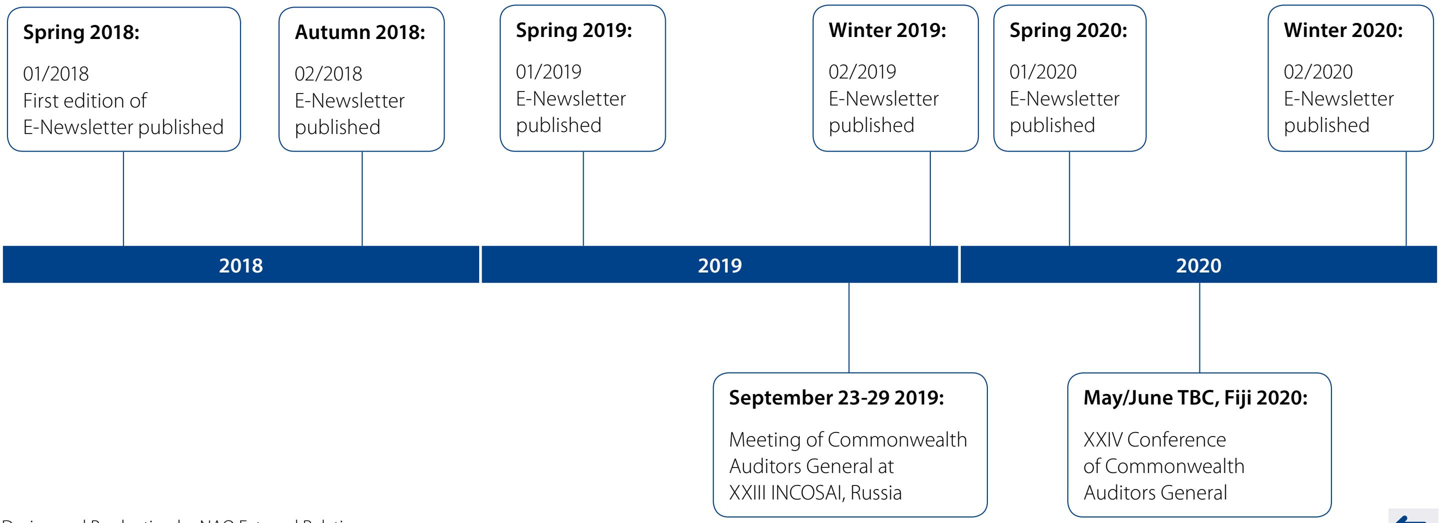
For more information contact:

Matthew Salik

Deputy Head of International Outreach at the Commonwealth Parliamentary Association UK (CPA UK): SALIKM@parliament.uk

Timeline of key milestones

See below for a timeline of key milestones until the next Commonwealth Auditors General Conference in Fiji (May/June 2020). The timescales for future editions of the e-newsletter have been linked to the future activity of the group, for example to document the outcomes of the next meeting of Commonwealth Auditors General at the INCOSAI XXIII in Russia, and to communicate information before and after the next conference in Fiji. SAIs are encouraged to express interest in suggesting future technical content of the e-newsletter.



Spring 2018:
01/2018
First edition of
E-Newsletter published

Autumn 2018:
02/2018
E-Newsletter
published

Spring 2019:
01/2019
E-Newsletter
published

Winter 2019:
02/2019
E-Newsletter
published

Spring 2020:
01/2020
E-Newsletter
published

Winter 2020:
02/2020
E-Newsletter
published

2018 2019 2020

September 23-29 2019:
Meeting of Commonwealth
Auditors General at
XXIII INCOSAI, Russia

May/June TBC, Fiji 2020:
XXIV Conference
of Commonwealth
Auditors General

Design and Production by NAO External Relations
DP Ref: 11699-001