Government Information Quarterly xxx (xxxx) xxxx

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand

Nik Thompson[a,*], Antony Mullins[a], Thanavit Chongsutakawewong[b]

[a] School of Management, Curtin University, Kent Street, Bentley, Western Australia 6102, Australia
[b] KPMG, 1 South Sathorn Rd, Yannawa, Sathorn Bangkok 10120, Thailand

ARTICLE INFO

Keywords:
E-government
Website
Information security
Australia
Thailand
Privacy

ABSTRACT

We present the first comprehensive audit and comparison of e-government website security in two countries. Australia was selected for its high level of e-government adoption, while Thailand was selected in contrast as a developing nation. Through our audit of 800 pages across 40 websites, we reveal numerous security vulnerabilities suggesting that the high adopters of e-government may not always be providing better protection to their citizens. Alarmingly, the most basic web security measure, the use of Hypertext Transfer Protocol Secure encryption was only used in half of Australian and one-third of Thai sites. Our methodology included content analysis of policies and encryption, followed by security vulnerability testing, to provide the first baseline data on these two countries. Statistical analysis suggests that far from being the benchmark for security, Australian e-government sites do not significantly differ from Thai sites in their vulnerability level. The implications of these findings are examined, and recommendations are made for practice. It is hoped that these insights into the current state of security provide a needed stimulus to focus more on the practical information security aspects of e-government.

1. Introduction

E-Government continues to be embraced by the global community as more public services transition online. Advances in ICT have enabled the delivery of new types of government services, through a variety of digital channels such as email, smartphones, tablets, and smart cards. Central to e-government is the ability to deliver government information and services to support business and the wider community citizens, while also saving time and reducing cost (Carter & Bélanger, 2005; Lofstedt, 2005).

Digital services promise to enhance processing of data and transactions, sharing of information between government departments, transparency between government and citizens, and trust between government and users (Alshehri & Drew, 2010). Indeed, there are numerous success stories of effective e-government implementation. For example, the city of New York has garnered a reputation for its e-government's design rationality and ease of use. After the 9/11 attack, the city fully utilized all of the technology at its fingertips to provide a wide range of flexible public services, aiding in recovery efforts and streamlining the integration between emergency services (Dawes, 2002).

However, many challenges must be overcome to secure government resources from information security threats (Zhou & Hu, 2008) as a result of the expectation of e-government systems to link to the broader internet. High profile data breaches, such as the 21.5 million personal social security records stolen in 2015 from the United States Office of Personnel Management (OPM) (Wagstaff, Eng, & DeLuca, 2015) have done little to enhance the acceptance of such services. It is unclear whether increased adoption of digital services by a government is supplemented by sufficient attention to the prevention of security breaches, and the possible public harm associated.

The United Nations E-government Development Index ranks Australia second out of 193 countries in the world (United Nations, 2018). As an early adopter, the Australian government prides itself on being a leader in the development of e-government services (Australian Government, 2018). Alarmingly, Australia is also the most targeted country in the Asia Pacific region for cybersecurity attacks (Cisco Systems, 2018). With 490 million digital citizen transactions being processed at federal and state government levels every year (Deloitte Access Economics, 2015), there is a clear need for appropriate security measures within e-government.

Members of the public have a reasonable expectation that their

* Corresponding author.
E-mail addresses: nik.thompson@curtin.edu.au (N. Thompson), Antony.Mullins@cbs.curtin.edu.au (A. Mullins), thanavit.cho@gmail.com (T. Chongsutakawewong).

https://doi.org/10.1016/j.giq.2019.101408
Received 8 March 2019; Received in revised form 31 July 2019; Accepted 13 September 2019

private data will be protected, but in reality, this expectation is not always met (Thompson, Ravindran, & Nicosia, 2015). Although the security of government web portals is a topical issue, no systematic or comparative security analysis has been conducted to date. To address this research gap, we report on a comprehensive audit of 800 government pages on 40 websites.

To provide a cross country perspective, Australia given its high ranking and early adoption of e-government development was studied, while Thailand was selected as a low-adoption country given its emergence as a developing nation with a focus on increasing Information Communication Technology (ICT) services.

Two research questions direct this examination of e-government security:

RQ1. What is the current state of government website security in Australia and Thailand?

RQ2. Are there significant country-level differences in website security?

We make several contributions through this study. Firstly, we provide the first comprehensive auditing of the state of information security in practice. Secondly, we conduct our audit in two countries representing high and low e-government adoption and provide comparative analysis. Thirdly, we detailed a methodology through which interested parties may conduct their own auditing. We also suggest a short-cut approach for those who wish to perform a faster benchmark. Finally, as our analysis reveals areas for improvement in policy and practice we present a detailed discussion of the possible causes of any issues and describe recommendations to assist practitioners.

2. Literature review

To understand the depth of prior research in e-government adoption and security, we conducted a systematic review to identify gaps in the current body of knowledge and identify opportunities for research. We followed a four-step approach to selecting the literature as recommended by Dyba, Dingsoyr, and Hanssen (2007). The first step involved identifying relevant studies using the Scopus online database as the primary reference resource. Scopus is one of the most well-respected services containing over 22,800 serial titles, and over 1.4 billion cited references (Elsevier, 2019). The initial search used the keywords "*electronic government" or "e-government"*.

The second step excluded literature based on the title (Dyba et al., 2007), since the initial search for e-government literature, yielded 12,841 items, it was necessary to remove non-relevant papers from this list. Further filtering was done in the third step, in which the paper abstracts were also reviewed. To further refine and frame the research, we included "adoption" and "security" keywords in our literature search, further reducing the number of articles to 3335. Of these over 3000 refereed publications, only 93 covered vulnerability, and only 71 included any mention of vulnerability assessment, while only 7 of these included empirical data. The results of this systematic review revealed that while e-government security is a popular topic with many thousands of mentions, research typically stops short of actually evaluating the state of security in practice. Furthermore, no study provides a comparison between countries or evidence of whether national developments in e-government adoption have been accompanied by commensurate developments in the domain of information security. The final step of our systematic review involved analysis of the full text of the related e-government security papers; which are discussed in the following sections.

2.1. E-government

Government information or services that exist in the digitalized form (Lindgren, Madsen, Hofmann, & Melin, 2019) or are delivered electronically (Yildiz, 2007) generally sit within the umbrella term e-government. Primarily e-government can increase communication between government and citizens (Bonsón, Royo, & Ratkai, 2015), and deliver many types of services ranging from healthcare (Anthopoulos, Reddick, Giannakidou, & Mavridis, 2016), tax and payment (Hung, Chang, & Yu, 2006), and visa applications (Tholen, 2010). While accessibility to information is key to success (Scott, DeLone, & Golden, 2016), the level of success is ultimately tied to the level of adoption by citizens.

2.2. E-government adoption

Though our literature search revealed articles dating back to 1994, e-government adoption has risen to prominence during the past ten years with the increasing transition to digital services. Research at the turn of the century identified ways for governments to adapt ICT services to help transform and deliver government information and services (Chen & Gant, 2001) while identifying technical, financial and legal barriers that governments need to address in preparation of e-government service adoption (Moon, 2002). Recent research has focused on government citizens willingness to interact and use e-government services, identifying trust (Bélanger & Carter, 2008; Teo, Srivastava, & Jiang, 2008), and the lack of support (Faulkner, Jorgensen, & Koufariotis, 2019) as barriers to the adoption of e-government services. Carter and Bélanger (2005) identified three factors that impact on the citizens likelihood to use e-government services, being 1) how easy a site or service is to use, 2) how compatible the site is with other sites and services, and 3) how trustworthy the site is in terms of internet security and trust in government.

Additionally, Carter and Bélanger (2005) identify trust as being a problematic barrier for governments to overcome while recognizing the importance of privacy statements. Moon (2002), also identified the use of security and noted the use of encryption as being a necessity for citizen participation in interactive functions such as online elections. Bertot, Jaeger, and Grimes (2010) explored the impact of e-government on cultural attitudes toward transparency and stressed the positive impact of ICT on transparency. Teo et al. (2008) identified that trust in government is significantly related to trust in e-government websites, but not related to general trust in technology, further highlighting that the difference in citizen opinion could depend on the kind of information transactions they conduct. Current research on e-government adoption commonly calls for further research in e-government security to identify vulnerabilities within e-government websites. Though, as we have seen, few researchers conduct the next step to gather this empirical data.

Attitudes toward e-government services in early adopter countries have been the research focus of many scholars. In the UK, Kolsaker and Lee-Kelley (2008) researched the attitudes concerning citizens adoption of e-government services; similarly, Gauld, Goldfinch, and Horsburgh (2010) identified that citizens in Australia and New Zealand were less likely to use transactional e-government services. The cultural difference was identified as a factor in adoption willingness in a comparative study between the US and Spain (Rufín, Bélanger, Molina, Carter, & Figueroa, 2014), while Shi (2006) studied the difference in terms of accessibility between e-government websites in China and Australia. Similar findings have been found in late adopter countries such as Zambia (Bwalya, Du Plessis, & Rensleigh, 2014), Thailand (Bhuasiri, Zo, Lee, & Ciganek, 2016) and India (Rana & Dwivedi, 2015).

Many studies exist on e-government adoption, a large cohort of scholars has identified that among the general usability and design issues (Byun & Finnie, 2010), trust and security are a potential barrier to the success of e-government service implementation (Liu & Carter, 2018). However, a gap exists in that very few studies have conducted security analysis tests on e-government websites to gauge the actual impact that security may have on government web services.

2.3. Related work

Zhao and Zhao (2010) to date have provided one of the most thorough assessments of government website security by assessing 51 state government websites in the US. Through web content analysis and security auditing, the study revealed that all of the tested websites had security flaws that could lead to the disclosure of IP address information and only 61% of sites used encryption. While they did not perform a comprehensive vulnerability test, it brings an interesting perspective on comparative analysis which is well aligned with the work described later in this paper. Moen, Klingsheim, Simonsen, and Hole (2007) also conducted a broad study, assessing 212 worldwide countries e-government websites, suggesting that 81.6% of the websites were vulnerable to either Cross-Site Scripting (XSS) or SQL (database) Injection; however, these results must be interpreted with caution due to methodological limitations including non-random sampling.

Awoleye, Ojuloge, and Siyanbola (2012) assessed five common web vulnerabilities in the form of SQL Injection, XSS, broken links, unencrypted passwords, and cookie manipulation across 64 Nigerian e-government websites. The findings indicated 42.2% of sites are susceptible to XSS vulnerabilities and 31.3% SQL Injection; a follow-up study two years later using the same sites revealed a reduction in vulnerabilities to 28.1% for XSS and 21.9% for SQL Injection (Awoleye, Ojuloge, & Ilori, 2014). The study did not analyze the use of privacy policies in the selected websites but recommended the adoption of policies to ensure verification and certification of e-government websites before public launch, to confirm their authenticity and improve citizens' trust. Ismailova (2017) assessed 55 websites in the Kyrgyz Republic and identified website vulnerabilities in the form of SQL Injection and XSS issues. The broad level overview highlighted that while only 4% of sites had critical vulnerabilities, all sites had low-level vulnerabilities. Alsmadi and Abu-Shanab (2016) performed penetration tests on 28 government websites in Jordan to detect Hypertext Transfer Protocol (HTTP) and Denial of Service (DoS) related vulnerabilities. However, the study failed to analyze the two most prevalent web vulnerabilities discussed above in other related research: SQL Injection and XSS.

Bissyandé et al. (2015) assessed the security vulnerability of 42 government websites in Burkina Faso and discovered that 54% of websites are delivered via content management systems such as Joomla, that when unpatched can leave the system vulnerable, to allow attackers to exploit. Murah and Ali (2018) used web security scanning tools to assess the security of 16 Libyan government websites, discovering that only 12.5% of sites had either a security policy or privacy policy. A related study also discovered that 75% of sites had transmission ports open that should have been closed, leading the authors to conclude that 15 of the 16 tested websites were unsafe (Ali & Murah, 2018).

The scarcity of empirical data on e-government security shows that while it is a popular topic for theorists, little is known about the state of security in practice. Consequently, evidence-based discussions or recommendations for improvement or development in this area are fewer still. All of the related work described used different tools and methodologies, had varied sample sizes and sometimes non-random sampling approaches. As each study focussed only on one country, it is impossible to make any meaningful comparisons.

Interestingly, with the exception of Zhao and Zhao (2010), all studies have focussed on countries that rank relatively low in the United Nations E-government Development Index (Thailand (73), Kyrgyzstan (91), Jordan (98), Libya (140) and Nigeria (143)) (United Nations, 2018). Thus, it is not known whether an increased level of e-government adoption will be met with a corresponding increase in security.

The following section describes our methodology and sampling approach for our audit of e-government pages from two countries. By selecting a country that is very high in e-government development and another that is relatively low, and applying identical methodology to each, we perform a cross-country analysis. Thus, in addition to providing the first country-level baseline data on these two countries, we provide insight into global trends and make recommendations for policy and practice.

3. Methodology

We employed a comprehensive, two-stage approach to data collection and analysis. Web content analysis of site policies and encryption was first undertaken, followed by a detailed information security audit to determine if the sites are vulnerable to security breaches. This methodology provided a rigorous and thorough evaluation of e-government website security. The following section details the data sample and the evaluation methodology.

3.1. Data sample and approach

E-government sites for both Australia and Thailand were initially drawn from the DMOZ online directory (DMOZ, 2019). As DMOZ proved to contain many broken links, a google search constrained to *.gov.au and *.go.th top-level domains supplemented this data sample. From the resulting list, 40 domains were randomly chosen and data collection was conducted in mid-2018.

The site auditing was conducted on 20 pages per e-government website across 40 domains, giving a total of 800 pages audited. The raw data collected during the audit directly address Research Question 1, to understand the state of e-government security. This data is then statistically tested to observe differences between groups. This statistical analysis addresses Research Question 2, which aims to find if there are differences between the countries.

3.2. Web content analysis

The web content analysis phase involved a manual assessment of e-government site content to catalogue the presence of privacy policies, and the use of encryption. Due to variance in site layouts and languages, this task was performed by a researcher fluent in both Thai and English. Web content analysis was undertaken by accessing the public web content of the e-government sites using the Mozilla Firefox web browser (version 64.0).

Privacy policies are the main area of interest; however, for informational purposes, several policies were documented. These include Security policy, Anti-hacking or misuse notice, Disclaimer of Liability and Terms of Use. The Australian site https://my.gov.au/ provided the exemplar. On this site, the home page provides links to Privacy, Terms of Use, and Security. In the Privacy page, details regarding the collection of personal information, the reasons of collecting the personal information, cookies, as well as further information such as how to access personal information held by the department, and seek the correction of that information is provided. As expected, this is in line with the Australian Privacy Act (Australian Government, 1988).

3.3. Information security audit

Information security auditing is conducted from the perspective of a potential attacker and involves an examination of security vulnerabilities. This phase is conducted to discover if flaws exist, which may present a security risk to the user or site administrator. It is a foundational step conducted by ethical hackers, in which harmless versions of many attacks are evaluated to ascertain if the system would be able to withstand a malicious attack of the same type. This form of auditing provides deep insights into overall security as actual live sites are tested.

Open Web Application Security Project, a not-for-profit organization, focuses its research projects on the security of web applications, identifying the top ten security risks (Open Web Application Security

Project, 2019), this provides a convenient baseline against which site security can be audited.

The information security audit phase was time-intensive even with the assistance of automated tools. During this type of auditing, thousands of web requests may be issued to test all possible configurations and inputs; thus, the network speed and computer resources pose a bottleneck which slows down the data collection. The data collection for this phase took approximately 720 computer hours in total, even though our tools were issuing multiple web requests concurrently.

Before commencing an audit, network mapping is first undertaken to learn what services (application version and name) the server is using and whether firewalls/packet filters are present. For this step, the industry-standard "Nmap" was used to scan the most common 1000 network ports on each of the 40 e-government sites (Kakareka, 2013).

To find the best resources for the job, we independently evaluated various auditing tools. In this evaluation, we performed audits of a small number of sites with eight different tools and selected those which provided the most thorough results. We tested: Acunetix, Wapiti, w3af, OWASP ZAP, Vega, Skipfish and Arachni, finding that only Arachni version 1.5.1 and OWASP Zed Attack Proxy (ZAP) 2.7.0 provide a comprehensive assessment. As our site auditing aimed to use the OWASP Top Ten Web Vulnerabilities list as a benchmark, it was appropriate to select ZAP 2.7.0 also developed by OWASP (Open Web Application Security Project, 2019).

3.4. Ethics

We tailored our methodology to ensure strict adherence with legal and ethical requirements. The Web content analysis phase was conducted manually within a regular web browser and posed no potential concerns. The information security auditing phase employed automated auditing tools and was carefully planned and executed. This was to ensure that the tools did not inadvertently overstep the simple information-gathering goal and that no detriment was caused to the sites being scanned.

Network mapping tasks have been covered in prior work (e.g. Zhao & Zhao, 2010) and the act of checking a network port's status does not constitute access to data. This type of scanning is now common as Internet-wide scans are routinely conducted (Rapid 7 Security, 2019). Nevertheless, we adopted the least intrusive approach possible: to only observe the open/closed status and not attempt to access services running on detected ports. Next, the vulnerability scanner was set up to passively test for the presence of vulnerabilities. Thus our method would simply inform whether a vulnerability is present and **not** whether it can be exploited. Our methodology included three protections; 1: **Prevent** access of any non-public or protected content by only scanning pages linked from the main homepage 2: **Passively** test for vulnerability by inspecting normal web traffic to ensure that no unauthorized access could occur and 3: **Limit** the speed and extent of scanning to ensure that sites did not experience detrimental or even noticeable load. At no point did our data collection bypass technical barriers or access any non-public-facing computers.

4. Results

4.1. Web content analysis

Australian sites generally fared well in terms of policy coverage, with most sites containing a privacy policy, disclaimer notice and security policy. Thai government websites showed more variance in the web content analysis, with no single policy appearing on more than half of the sites tested. Table 1 provides a summary of the analysis of site policies.

The results for encryption use were alarming as only 50% of Australian sites forced the use of encryption in the form of the HTTPS protocol. Thai sites also fared badly on the encryption test as only 35% of sites forced the use of HTTPS. Some sites provided optional encryption by running both HTTP and HTTPS accessible sites. Unfortunately, in most cases, the optionally encrypted version of the site was misconfigured introducing further vulnerabilities.

Table 1
Analysis of site policies.

Category	Country			
	Australia		Thailand	
	Number	Percent	Number	Percent
Privacy Policy	20	100%	8	40%
Disclaimer	19	95%	9	45%
Security Policy	17	85%	8	40%
Terms of use	1	5%	9	45%

4.2. Information security audit

Network mapping was undertaken to discover the status of the most common 1000 ports. This revealed that 17 distinct ports were open across the Australian sites tested, and 23 on the Thai sites. Many of these are "well known" ports which correspond to common services and are managed by the Internet Assigned Numbers Authority. No critical issues were noted during the network mapping.

The information security auditing results are organized into high, medium and low severity alerts. All sites generated some alerts, as some low severity alerts are informational and therefore frequent. In the Australian sample 45% of sites generated high severity alerts, 75% generated medium severity alerts and all sites generated low severity alerts. For the Thai sample, 60% generated high severity alerts, 65% medium severity and again all sites generated low severity alerts. Fig. 1 summarizes the percentage of affected sites for each class of vulnerability.

4.3. Cross country comparison

To address Research Question 2, statistical analysis was undertaken to understand whether any apparent differences between countries were significant. As this data was categorical, the Pearson χ^2 (chi-squared) test was used to evaluate whether any apparent differences between the categorical data sets are real or if they could arise by chance.

This test revealed that a significantly larger number of Australian websites provided privacy policy information ($\chi^2 = 17.143$, df = 1, $p < .05$). For the test of HTTPS encryption, both Australian and Thai sites demonstrated a low usage. There was no statistically significant difference between the two countries ($\chi^2 = 0.921$, df = 1, $p = .337$). Finally, there was no statistically significant difference in the number of

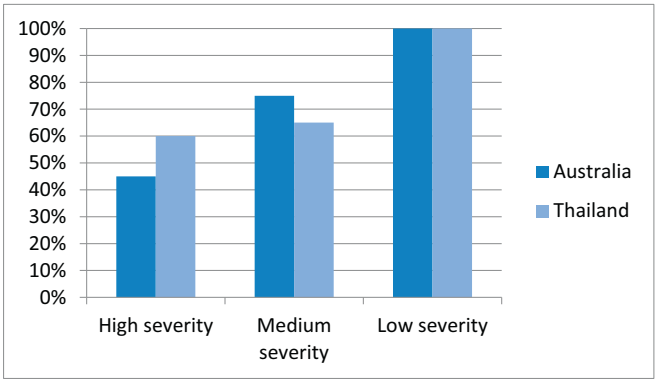

Fig. 1. Vulnerability scan results.

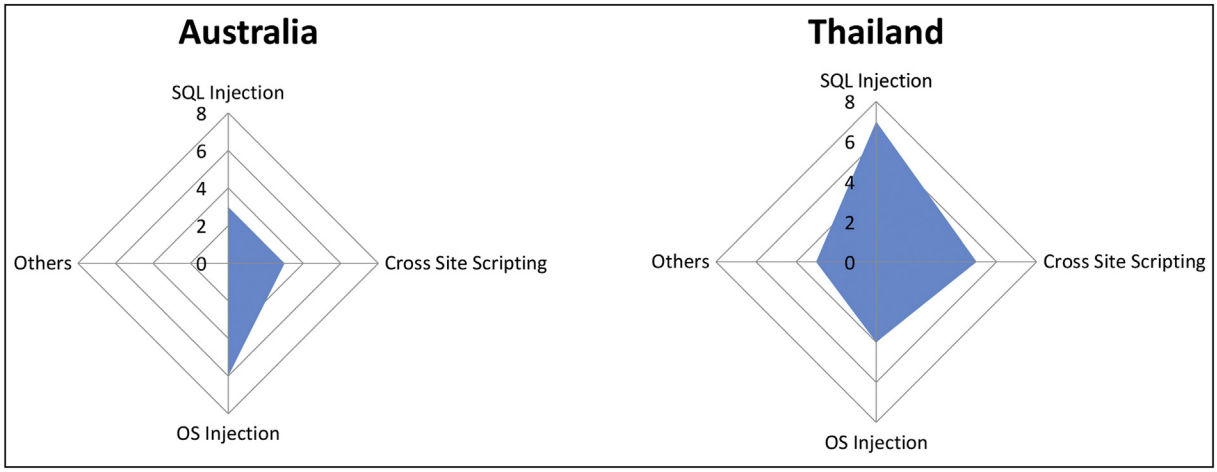

Fig. 2. Vulnerability profile of Australia vs Thailand

high severity vulnerabilities between Australia and Thailand ($\chi^2 = 0.902$, df = 1, $p = .342$).

5. Analysis

5.1. Web content analysis

Universal uptake of privacy policies in Australian sites indicated that this is now a well-understood requirement and is standard fare for a government site. At the other end of the spectrum, terms of use are rarely found. It is possible that the Australian government might think their citizens know how to use the website in general terms which explains the absence of terms of use. Thai results appeared worse for every policy category tested with less than half of the sites containing any given policy. Furthermore, in some cases, names of policies were present, but these were merely placeholders which did not link to any actual content. In one site, the link to the security policy was broken, so it was not possible to ascertain if it existed. The absence of site policies, particularly privacy policies could be a symptom of the lack of legislative influence.

Though differences in policy coverage between Australia and Thailand were apparent, findings converged when encryption usage was tested. Sites using Hypertext Transfer Protocol (HTTP) as opposed to the encrypted HTTPS standard are considered a security risk due to the possibility of exposing sensitive data (Franks et al., 1999). Unencrypted connections can be vulnerable to interception, eavesdropping, tracking, and modification along with impersonation of websites (Gastellier-Prevost, Granadillo, & Laurent, 2011) to gain access to user data such as “browser identity, website content, search terms, and other user-submitted information” (Common Weakness Enumeration, 2019b). Sites from both countries demonstrated a low adoption of HTTPS encryption and were not statistically different from one another.

Only half of Australian and one-third of Thai sites forced the use of encryption; others either forced the insecure HTTP or provided both options, leaving room for what are known as “downgrade attacks” in which attackers target the least secure protocol available (Alashwali & Rasmussen, 2018). Further investigation also revealed technical deficiencies in the form of misconfiguration. Five Australian sites which did not force encryption provided it as an option, yet these contained misconfigurations such as expired or invalid certificates leading to a browser error.

This situation was repeated in the Thai sites, where out of those which provided optional encryption, all but one site was misconfigured rendering them insecure. If these HTTPS sites are being run in parallel with the HTTP sites to eventually switch over to HTTPS encryption, some concerted effort is required to properly configure them. In some cases, the misconfigurations are extremely severe; for instance, one site had a certificate which had expired a decade prior in February 2009. Another site used a certificate which was registered for an entirely different purpose: to certify non-Thai websites used for football and gaming.

5.2. Information security audit

Three types of high severity vulnerabilities were detected in sites from both Australia and Thailand. These vulnerabilities, if exploited can lead to near-complete compromise of confidentiality and integrity of data on the target machine. These were OS Command Injection, SQL Injection, and Cross-Site Scripting.

OS Command Injection occurs when a command running on the web server utilizes some user-supplied input but does not perform adequate checks to ensure that this input is safe. This vulnerability may lead to an attack where an attacker can run commands on the target web server (Common Weakness Enumeration, 2019a).

SQL Injection vulnerabilities arise when user input is delivered to a database (SQL) server, without adequately checking to ensure its safety. A successful attack will enable the attacker to access secure data from the database, modify individual records or execute operations on the database such as shutdown or deletion of the entire database. As such, SQL injection attacks can be especially dangerous (Open Web Application Security Project, 2019).

Cross-Site Scripting (XSS) attacks can occur when the web site accepts user-supplied input but does not perform sufficient checking before this input is then served to other users. XSS attacks may allow an attacker to upload a malicious script, which is then unwittingly served to other users as part of the web site's regular operation. The malicious script may steal private data, cookies or trick users into entering credentials which may lead to compromised accounts on that website or others which may share those credentials (Common Weakness Enumeration, 2019b).

The vulnerability profile of Australia vs Thailand differs in that a few additional vulnerabilities were detected only on Thai sites, and the prevalence of particular vulnerabilities are dissimilar. The most pressing concern is SQL Injection, affecting a third of Thai sites. The vulnerability profiles are illustrated below in Fig. 2 showing how sites from both countries are affected by several classes of high severity issue:

6. Discussion

6.1. What is the current state of government website security in Australia and Thailand?

Our first research question asked: *What is the current state of government website security?* Through this, we address the lack of empirical research and provide the first baseline data on two countries. Our audit revealed numerous security vulnerabilities in sites from both Australia and Thailand. We conclude that the current state of government website security needs improvement in both countries.

Firstly, the web content analysis suggests a large amount of variance in the type of policies displayed on e-government sites. All Australian sites present privacy policy as a minimum baseline,this is in line with legislative requirements and the Australian Privacy Act of 1988 (Australian Government, 1988). However, other policies are not always present.

For Thai sites, the distribution is unusual in that there are some sites which contain all of the policies and others which contain none at all, showing a lack of consistency and standardization in the development of websites. Our data suggest that Thai sites do not emphasize protection of data or privacy to their site visitors, perhaps due to a lack of legislative influence. Cybersecurity, and personal data protection legislation has been approved in principle, to protect public and private data (National News Bureau of Thailand, 2018; The Nation, 2018). This legislation is an important step that the Thai government can take to protect its citizens.

The analysis of HTTPS encryption revealed some concerning results, as this fundamental and easily implemented form of security protection is not widely adopted. Only half of the Australian sites and one-third of the Thai sites forced the use of HTTPS encryption. In addition, some sites contained severe misconfigurations such as expired certificates (some by more than a decade) or registration to different sites altogether. This is unacceptable, given that HTTPS encryption is supported on all modern computers and mobile devices. This figure is in contrast to the US Federal Government who lead the world with 74% adoption of HTTPS (United States Government, 2019a), exceeding the HTTPS adoption in the broader internet. Their success can be attributed to a combination of legislation in the form of the HTTPS-Only Standard (United States Government, 2019b), and transparency, as compliance of federal government websites is publicly displayed.

Secondly, the information security audit revealed high, medium and low severity issues in both countries' websites with around half of all sites containing potential high severity issues. Among these, Operating System or Database injection attacks and Cross-Site Scripting appear prominently in both the Australian and Thai results. This finding is consistent with global statistics, as these three vulnerabilities are among the most critical web security risks (Open Web Application Security Project, 2019). In addition, several further high severity issues were found only in Thai sites.

6.2. Are there any significant country-level differences in website security?

Our second research question asked: *Are there any significant country-level differences in website security?* We only found significant cross-country differences in one category: privacy policy. Other results for HTTPS encryption and high severity vulnerabilities did not yield statistically significant differences. That is to say, that rather than setting the benchmark for high-security, sites from the high e-government adopter Australia were plagued by an alarming number of potential issues rendering them no more secure than their Thai counterparts. These findings are summarised in Table 2.

Though not statistically significant, based on raw counts of vulnerabilities, it initially seemed that Thai sites had fared worse than their Australian counterparts. In general, there was a higher percentage of affected Thai sites, as well as a greater range of issues detected in the Thai sites. As several of these issues are easily addressed by following industry best practices during site development, it appeared that the Thai web developers were simply not following these industry standards. This may be a result of the fact that industry best-practices typically originate from the United States (Open Web Application Security Project, 2019; Spitzner, 2018) and are generally published in English. This valuable information is thus less widely accessible to non-English speaking communities.

6.3. Implications

Our findings have several implications for practitioners and policymakers as we identify areas for improvement of e-government resources. These can be addressed through three recommendations.

6.3.1. Legislation

Local legislation is a driver of security implementation, as systems must comply with relevant laws. Therefore some of the differences between the countries may likely stem from the level of maturity of public policy and legislation. While Australia has personal data protection laws in place, many developing countries are yet to publish policies and legislation.

Stemming from the Australian Privacy Act of 1988 (Australian Government, 1988), the Australian Privacy Principles deal with the collection, disclosure, integrity, and access to personal information (Australian Government, 1988). Thailand, however, does not yet have laws to regulate personal data collection and protection. Thailand's government cabinet approved the first personal data protection act draft in May 2018 (Boonklomjit, Rerknithi, Gamvros, & Kwok, 2018), with approval in principle from the National Legislative Assembly received in December of that year (National News Bureau of Thailand, 2018). The legislation is now awaiting approval from His Majesty the King of Thailand (Suwanprateep, Paiboon, & Tongkak, 2018).

Legislation has proved to be a positive influence on e-government, seen in our data on Australian sites with 100% including a privacy policy. The Thai government would be well advised to finalize privacy laws so websites can inform their users and in turn protect citizens and businesses. The Australian government would also be advised to learn from the success of the US government in applying HTTPS as a standard. The US House Office of Management and Budget memorandum M-15-13, had a direct impact on government websites use of HTTPS (United States Government, 2019b), providing further evidence that legislation can have a positive effect.

6.3.2. Standard government web platform

A template-based approach should be adopted, using a common government web platform and template which meets usability, consistency and security requirements. Given that government websites share common themes and target the same audience, Molich and Nielsen (1990) best practice principles could be applied in terms of design consistency. Our study identified a broad range of site designs in terms of the look and feel of the websites. Thai government websites showed a larger variance from site to site, and pages often displayed private web developers contact details, suggesting web development is outsourced, furthering the lack of design consistency. Templates could assist in ensuring the accuracy of content, and could be delivered through a content management system, leading to an improvement in security administration and a reduction in the maintenance and cost of web development (Han, 2004). In addition to templating, routine site audits should be scheduled. Such site auditing would both alert administrators to the security issues found in our audit, and also aid in the identification of usability issues; leading to an overall improvement in experience for site visitors.

6.3.3. Accessibility of industry standards

Only the major industry standards such as ISO/IEC 27002

Table 2
Comparison between Australia and Thailand.

Category	Country				χ^2	Probability	Sig?
	Australia		Thailand				
	Number	Percent	Number	Percent			
Privacy policy	20	100%	8	40%	17.143	$p < .05$	✓
Encryption	10	50%	7	35%	0.921	$p = .337$	✗
High severity vulnerabilities	9	45%	12	60%	0.902	$P = .342$	✗

(International Organization for Standardization, 2013) are available in multiple languages. However, the ISO/IEC 27002 (International Organization for Standardization, 2013) is not a standalone solution to security (Chapple, 2012). Other important practitioner reports such as OWASP are published in English and are yet to be translated into Thai (Open Web Application Security Project, 2019; Spitzner, 2018). Therefore a concentrated effort on the translation of industry standards may boost conformance internationally. The lack of resources in the local language may be a barrier to the uptake of security best practices, and this may have contributed to some of the additional issues discovered in the Thai sites, a finding that is likely to extend to other non-western and developing countries.

6.4. Limitations and future work

Our auditing considered a sample of 800 pages on 40 e-government websites. These were randomly selected to eliminate systematic bias in the measurement, and it is assumed that the randomly chosen sample is representative of all similar sites. However, a different or larger sample may yield different outcomes from the auditing phase, and this should be taken into account when attempting to generalize the findings.

The information security auditing process infers the presence of vulnerabilities by issuing crafted web-requests and analyzing the website response. For ethical and legal reasons, our auditing methodology did not attempt to exploit these potential vulnerabilities. Therefore, the results of the audit may be susceptible to Type I error. However, as the same methodology and tools were used for all sites, the cross-country comparison is considered to be robust. Furthermore, the web content analysis does not suffer from this limitation. Future work could involve collaboration with relevant government agencies to extend the testing methodology to include deeper vulnerability testing and exploitation.

Our method is replicable and we invite other researchers to continue this work in different countries. Although our auditing process is time-consuming, we believe that the most accurate results will be gleaned through applying it intact. However, a potential short-cut approach for those who are interested in a quick benchmark would be to scan only for the three classes of vulnerabilities that are more likely to appear. These are OS Command Injection, SQL Injection and Cross-Site Scripting which, as discussed earlier, were found in both Australian and Thai e-government sites. Another viable benchmark is to repeat only the web content analysis phase. This only requires a web browser and no special tools, and will still give useful insights into the policy and encryption status of the sites.

Finally, prior work has shown that national culture influences the design of government websites (Alexander, Thompson, & Murray, 2017) due to shared norms and beliefs. It is possible that these culturally influenced design preferences may interact with security best-practices. Therefore another potential stream of research is to consider if and how the security of websites is culturally influenced.

7. Conclusion

We set out to discover if a high level of e-government adoption was accompanied by a commensurate level of security development. To this end, we conducted security audits in two countries globally ranked low and high in terms of e-government adoption. Though the low adopter's security appeared superficially worse, these differences were not statistically significant from the high adopter. This may reflect an environment in which service delivery, not security, is a key metric of adoption. Focussing on narrow targets may provide a narrow perspective on broader system *success*. Indeed, in some cases, high adoption figures may have been bolstered by a push toward migrating existing services to digital form without addressing the potential security risk faced by the public.

It is of concern that e-government adoption is not being accompanied by sufficient attention and investment in security and data protection. In light of the recent targeting of government entities by cybercriminals (Liska, 2019), this is a situation that must be addressed as a priority. The crucial first step is for government departments to commission their own security audits and discover any vulnerabilities before malicious actors do the same. They may find our methodology useful in this regard.

What then, of the prior research suggesting that security concerns would be a barrier to high adoption?

The answer may lie in the extent to which the use of e-government is either mandated or voluntary for citizens. While security and other barriers to adoption are crucial for voluntary use of public services, many services are forced upon the public through the removal of the traditional paper-based or in-person approaches. Once again, a narrow focus on service delivery levels might provide only a partial representation of system success.

Take, for example, Australia's rollout of electronic health records. Launched in 2012 as an opt-in service, the uptake for this ostensibly beneficial service was so low that after four years, only 10% of the population had signed up for the billion-dollar initiative (Gartrell, 2015). Following a legislative change to force the creation of this health record for all citizens, there was extensive media attention and petitioning which culminated in millions of citizens requesting to be removed from the program, many citing concerns about their security (King, 2019). Security concerns and public trust are clearly an issue for the success of e-government initiatives.

Government agencies have the opportunity to be champions of data security and accountability - something particularly desirable in this age of big and open linked data (Janssen & Kuk, 2016). Rather than taking a reactive approach to data issues, government agencies may set the standard to which private and public sector alike strive to attain. Thus the central question for public sector agencies should not simply be whether public services can be transitioned to new digital platforms, but rather how these can be the most effective and useful for citizens. Taking appropriate steps to safeguard the security of citizens' data, and being seen to do so would lead to a more usable and reliable environment which would enhance public trust, and ultimately lead to greater acceptance and use of e-government services.

References

Alashwali, E. S., & Rasmussen, K. (2018). What's in a downgrade? A taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS.

Proceedings of the International Conference on Security and Privacy in Communication Systems.
Alexander, R., Thompson, N., & Murray, D. (2017). Towards cultural translation of websites: a large-scale study of Australian, Chinese, and Saudi Arabian design preferences. *Behaviour & Information Technology, 36*(4), 351–363.
Ali, A. A., & Murah, M. Z. (2018). Security Assessment of Libyan Government Websites. *Proceedings of the 2018 Cyber Resilience Conference*. CRC.
Alshehri, M., & Drew, S. (2010). Implementation of e-government: advantages and challenges. *Proceedings of the International Association for Scientific Knowledge*. IASK.
Alsmadi, I., & Abu-Shanab, E. (2016). E-government website security concerns and citizens' adoption. *Electronic Government, an International Journal, 12*(3), 243–255.
Anthopoulos, L., Reddick, C. G., Giannakidou, I., & Mavridis, N. (2016). Why e-government projects fail? An analysis of the Healthcare. gov website. *Government Information Quarterly, 33*(1), 161–173.
Australian Government (1988). Privacy Act 1988. Retrieved 2 Nov, 2018, from https://www.legislation.gov.au/Series/C2004A03712.
Australian Government (2018). Australia's Tech Future - Delivering a strong, safe and inclusive digital economy. Retrieved 1 Feb, 2019, from https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf.
Awoleye, M. O., Ojuloge, B., & Ilori, M. O. (2014). Web application vulnerability assessment and policy direction towards a secure smart government. *Government Information Quarterly, 31*, S118–S125.
Awoleye, M. O., Ojuloge, B., & Siyanbola, W. O. (2012). Technological assessment of e-government web presence in Nigeria. *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*.
Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165–176.
Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27*(3), 264–271.
Bhuasiri, W., Zo, H., Lee, H., & Ciganek, A. P. (2016). User acceptance of e-government services: examining an e-tax filing and payment system in Thailand. *Information Technology for Development, 22*(4), 672–695.
Bissyandé, T. F., Ouoba, J., Ahmat, D., Ouédraogo, F., Béré, C., Bikienga, M., & Sié, O. (2015). Vulnerabilities of government websites in a developing country–the case of Burkina Faso. *Proceedings of the international conference on e-infrastructure and e-services for developing countries*.
Bonsón, E., Royo, S., & Ratkai, M. (2015). Citizens' engagement on local governments' Facebook sites. An empirical analysis: The impact of different media and content types in Western Europe. *Government Information Quarterly, 32*(1), 52–62.
Boonklomjit, H., Rerknithi, N., Gamvros, A., & Kwok, R. (2018). Overview of Thailand Draft personal data protection act. Retrieved January 6, 2019, from https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/.
Bwalya, K. J., Du Plessis, T., & Rensleigh, C. (2014). E-government implementation in Zambia–prospects. *Transforming Government: People, Process and Policy, 8*(1), 101–130.
Byun, D.-H., & Finnie, G. (2010). Evaluating usability, user satisfaction and intention to revisit for successful e-government websites. *Electronic Government, an International Journal, 8*(1), 1–19.
Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5–25.
Chapple, M. (2012). Can ISO 27002 be used as a standalone guide for security management? Retrieved January 5, 2019, from https://searchsecurity.techtarget.com/answer/Can-ISO-27002-be-used-as-a-standalone-guide-for-security-management.
Chen, Y.-C., & Gant, J. (2001). Transforming local e-government services: the use of application service providers. *Government Information Quarterly, 18*(4), 343–355.
Cisco Systems (2018). Cisco 2018 Asia Pacific Security Capabilities Benchmark Study. Retrieved 1 Nov, 2018, from https://www.cisco.com/c/dam/global/en_au/products/pdfs/cisco_2018_asia_pacific_security_capabilities_benchmark_study.pdf.
Common Weakness Enumeration (2019a). CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection'). Retrieved January 22, 2019, from https://cwe.mitre.org/data/definitions/77.html.
Common Weakness Enumeration (2019b). CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). Retrieved January 22, 2019, from https://cwe.mitre.org/data/definitions/89.html.
Dawes, S. S. (2002). The future of e-government. *Center for Technology in Government*. University at Albany.
Deloitte Access Economics (2015). Digital government transformation. Retrieved 2 Feb, 2019 from https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-digital-government-transformation-230715.pdf.
DMOZ (2019). DMOZ - The directory of the web. Retrieved 2018, 1 June, from http://dmoz-odp.org/.
Dyba, T., Dingsoyr, T., & Hanssen, G. K. (2007). Applying systematic reviews to diverse study types: An experience report. *Proceedings of the First International Symposium on Empirical Software Engineering and Measurement*. 2007: ESEM.
Elsevier (2019). Scopus. Retrieved 18th June, 2019, from https://www.elsevier.com/solutions/scopus/how-scopus-works/content.
Faulkner, N., Jorgensen, B., & Koufariotis, G. (2019). Can behavioural interventions increase citizens' use of e-government? Evidence from a quasi-experimental trial. *Government Information Quarterly, 36*(1), 61–68.
Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., & Stewart, L. (1999). HTTP authentication: Basic and digest access authentication (2070–1721). Retrieved from https://www.ietf.org/rfc/rfc2617.txt.
Gartrell, A. (2015). Australians to benefit from Sussan Ley's ehealth health records revamp. Retrieved from https://www.smh.com.au/politics/federal/australians-to-benefit-from-sussan-leys-ehealth-health-records-revamp-20150508-ggxkew.html.
Gastellier-Prevost, S., Granadillo, G. G., & Laurent, M. (2011). Decisive heuristics to differentiate legitimate from phishing sites. *Proceedings of the 2011 Conference on Network and Information Systems Security (SAR-SSI), La Rochelle, France*.
Gauld, R., Goldfinch, S., & Horsburgh, S. (2010). Do they want it? Do they use it? The "Demand-Side"of e-Government in Australia and New Zealand. *Government Information Quarterly, 27*(2), 177–186.
Han, Y. (2004). Digital content management: the search for a content management system. *Library Hi Tech, 22*(4), 355–365.
Hung, S.-Y., Chang, C.-M., & Yu, T.-J. (2006). Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. *Government Information Quarterly, 23*(1), 97–122.
International Organization for Standardization (2013). *ISO/IEC 27002:2013 - Information technology Security techniques - Code of practice for information security controls*.
Ismailova, R. (2017). Web site accessibility, usability and security: a survey of government web sites in Kyrgyz Republic. *Universal Access in the Information Society, 16*(1), 257–264.
Janssen, M., & Kuk, G. (2016). Big and open linked data (BOLD) in research, policy, and practice. *Journal of Organizational Computing and Electronic Commerce, 26*(1–2), 3–13.
Kakareka, A. (2013). What is vulnerability assessment? *Managing Information Security* (pp. 201–221). Elsevier.
King, C. (2019). More than 2.5 million Australians opt out of my health record. Retrieved 7 March, 2019, from https://www.catherineking.com.au/2019/02/20/more-than-2-5-million-australians-opt-out-of-my-health-record/.
Kolsaker, A., & Lee-Kelley, L. (2008). Citizens' attitudes towards e-government and e-governance: a UK study. *International Journal of Public Sector Management, 21*(7), 723–738.
Lindgren, I., Madsen, C., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A research agenda for the digitalization of public services. *Government Information Quarterly. 36*(3), 427–436.
Liska, A. (2019). Early findings: review of state and local government ransomware attacks. Retrieved 9 July, 2019, from https://www.recordedfuture.com/state-local-government-ransomware-attacks/.
Liu, D., & Carter, L. (2018). Impact of citizens' privacy concerns on e-government adoption. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*.
Lofstedt, U. (2005). E-government-assesment of current research and some proposals for future directions. *International journal of public information systems, 1*(1), 39–52.
Moen, V., Klingsheim, A. N., Simonsen, K. I. F., & Hole, K. J. (2007). Vulnerabilities in e-governments. *International Journal of Electronic Security and Digital Forensics, 1*(1), 89–100.
Molich, R., & Nielsen, J. (1990). Improving a human-computer dialogue. *Communications of the ACM, 33*(3), 338–348.
Moon, M. J. (2002). The evolution of e-government among municipalities: rhetoric or reality? *Public Administration Review, 62*(4), 424–433.
Murah, M. Z., & Ali, A. A. (2018). Web assessment of libyan government e-government services. *International Journal of Advanced Computer Science and Applications, 9*(12), 583–590.
National News Bureau of Thailand (2018). NLA approves in principle bills related to public health. Retrieved January 6, 2019, from http://nwnt.prd.go.th/CenterWeb/NewsEN/NewsDetail?NT01_NewsID=WNSOC6112290010006.
Open Web Application Security Project (2019). OWASP Top Ten Project. Retrieved October 26, 2018, from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#Translation_Efforts_2.
Rana, N. P., & Dwivedi, Y. K. (2015). Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT). *Government Information Quarterly, 32*(2), 172–181.
Rapid 7 Security (2019). Project Sonar. Retrieved, from https://opendata.rapid7.com/about/.
Rufín, R., Bélanger, F., Molina, C. M., Carter, L., & Figueroa, J. C. S. (2014). A cross-cultural comparison of electronic government adoption in Spain and the USA. *International Journal of Electronic Government Research (IJEGR), 10*(2), 43–59.
Scott, M., DeLone, W., & Golden, W. (2016). Measuring eGovernment success: a public value approach. *European Journal of Information Systems, 25*(3), 187–208.
Shi, Y. (2006). E-government web site accessibility in Australia and China: A longitudinal study. *Social Science Computer Review, 24*(3), 378–385.
Spitzner, L. (2018). Looking For Translators. Retrieved January 25, 2019, from https://www.sans.org/security-awareness-training/blog/looking-translators.
Suwanprateep, D., Paiboon, P., & Tongkak, K. (2018). Thailand: Cybersecurity Bill Revised and Reissued in November 2018. Retrieved January 6, 2019, from https://globalcompliancenews.com/thai-cybersecurity-bill-revised-november-2018-20181220.
Teo, T. S., Srivastava, S. C., & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of Management Information Systems, 25*(3), 99–132.
The Nation (2018). Cybersecurity, data protection bills await NLA approval. Retrieved January 6, 2019, from http://www.nationmultimedia.com/detail/national/30360686.
Tholen, B. (2010). The changing border: developments and risks in border control management of Western countries. *International Review of Administrative Sciences, 76*(2), 259–278.
Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly, 32*(3), 316–322.
United Nations (2018). UN E-Government Knowledgebase. Retrieved 26th June, 2019, from https://publicadministration.un.org/egovkb/en-us/data/compare-countries.
United States Government (2019a). Pulse. Retrieved February 6, 2019, from https://

pulse.app.cloud.gov/https/domains/.
United States Government (2019b). The HTTPS-Only Standard. Retrieved January 4, 2019, from https://https.cio.gov/.
Wagstaff, K., Eng, J., & DeLuca, M. (2015). OPM: 21.5 million people affected by background Check Breach. Retrieved January 21, 2019, from https://www.nbcnews.com/tech/security/opm-hack-security-breach-n389476.
Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly, 24*(3), 646–665.
Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*(1), 49–56.
Zhou, Z., & Hu, C. (2008). Study on the e-government security risk management. *International Journal of Computer Science and Network Security, 8*(5), 208–213.

Nik Thompson is a Senior Lecturer in Information Systems at Curtin University, Australia. He holds MSc and PhD degrees and works in the area of Computer Security and Information Systems. His research interests include affective computing, human-computer interaction and information security. His work has appeared in various journals including Government Information Quarterly, Computers & Security and Behavior and Information Technology.

Antony Mullins is an Associate Lecturer in the School of Management at Curtin University, Australia. He holds an MCom degree and works in the area of Information Technology and Information Systems. He is currently a PhD candidate working in the area of Information Technology and Big Data. His other research interests include information security and computer networks.

Thanavit Chongsutakawewong is a Senior IT Auditor at KPMG Thailand. He holds a Master of Information Systems from Curtin University. His current role includes IT audit engagement for corporate clients including testing information security controls, systems change management, system development and computer operations. His interests include cyber security, network security and advanced technologies.