Western Australian
Auditor General's Report

Cyber Security in Local Government

Report 9: 2021-22

24 November 2021

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Ben Goodwin
Reshma Vikas
Jordan Langford-Smith

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL’S REPORT

Cyber Security in Local Government

Report 9: 2021-22
November 2021

This page intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

CYBER SECURITY IN LOCAL GOVERNMENT

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

This audit assessed if a sample of 15 local government entities manage cyber security risks and respond to cyber threats effectively.

I wish to acknowledge the entities' staff, my Information Systems Audit team, and the staff and students at Edith Cowan University's Security Research Institute for their cooperation and expertise with this audit.

CAROLINE SPENCER
AUDITOR GENERAL
24 November 2021

Contents

Auditor General's overview

Western Australian local government (LG) entities are increasingly using online services to connect with their communities and conduct government business. Alongside the many benefits that arise from this digital connectivity are just as many, if not more, risks. None more challenging than the attempts of cybercriminals to gain unlawful access to government systems and information, disrupting supply chains and services. The number of cyber-attacks across government rose sharply during the COVID-19 pandemic and will continue to present challenges for governments who are entrusted with citizen information and ongoing delivery of essential services.

LG entities use key systems to deliver services to their communities and in doing so collect and store vast amounts of information about their residents and operations. This information is attractive to cybercriminals. LG entities need to understand and mitigate their cyber security risks. In doing so, entity capability and public confidence in digital initiatives and government processes will be strengthened.

This report summarises important findings and recommendations from our cyber security audit at 15 LG entities. Through our examination of control frameworks and ethical simulated cyber-attacks (ethical hacking), we found that LG entities had not managed their cyber security risks well. Out-of-date software accounted for a large number of cyber security vulnerabilities and despite staff awareness training, over half of the audited LG entities did not have controls to prevent their staff falling victim to social engineering attacks (for example phishing emails). Most of the LG entities we audited also lacked appropriate incident response and recovery plans to respond to cyber security incidents and recover key systems. LG entities must fix these weaknesses and improve their cyber security maturity.

LG entities should give regard to good practice principles in the Australian Government Information Security Manual and the Essential Eight controls to protect systems and information. While remediations will require an investment of time and money, support from senior management is equally important to uplift cyber security maturity. We have included recommendations and better practice guidance at Appendix 1 to help entities manage and address their cyber risks.

It was encouraging to see that most of the audited LG entities addressed some of our findings during the audit. All State and LG entities should take note of the findings and recommendations in this report.

Introduction

In this audit we assessed if a sample of 15 Western Australian LG entities manage cyber security risks and respond to cyber threats effectively. Appropriate management and response make it harder for cybercriminals to infiltrate LG entity networks to disrupt and compromise the confidentiality, integrity and availability of their systems and information.

LG entities manage vast amounts of operational information as well as personal information about their staff and communities. It is important that key systems and information are protected from internal and external malicious attacks. Cyber security is an essential part of that protection.

We have anonymised weaknesses and graphics throughout this report so as not to compromise the security of systems and information at the LG entities we audited.

Background

Australian government entities and organisations are constantly targeted in cyber-attacks aimed to unlawfully obtain information and disrupt essential services. The Australian Cyber Security Centre received over 67,500 reports of cyber security incidents in 2020-21, an increase of nearly 13% from the previous year. Government entities accounted for 35% of these incidents. Self-reported losses from cybercrime totalled more than $33 billion.[1] Earlier in 2021 cyber security incidents disrupted the Western Australian Parliament's emails[2] and Queensland's essential healthcare services.[3] Cyber security is one of the most significant issues facing organisations worldwide.

To manage their cyber security risks, we expected LG entities to have:

1. a cyber security policy and framework
2. a cyber security incident response plan
3. processes to manage cyber risks
4. cyber security awareness training for employees
5. intrusion detection and prevention systems
6. processes to manage technical vulnerabilities
7. a disaster recovery plan
8. a business continuity plan.

During the audit, we examined policies and procedures and carried out black box[4] simulated cyber-attacks and sent test phishing emails to assess LG entities' cyber security controls and defences. These approaches simulated real outside-in scenarios and without inside knowledge of the LG entities. The phishing emails contained non-malicious links designed to collect basic information, if opened, such as the network, user and operating system details. LG staff were then redirected to a website that asked for their username and password. We tested if entity controls could prevent phishing emails and whether appropriate security

[1] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (current as at 22/11/2021)

[2] https://www.abc.net.au/news/2021-03-17/wa-parliament-targeted-cyber-attack/13253926 (current as at 22/11/2021)

[3] https://ia.acs.org.au/article/2021/australian-hospitals-hit-by-cyber-attack.html (current as at 22/11/2021)

[4] The black box approach is used to simulate a real world scenario where tests are undertaken without any inside knowledge of the organisation's IT environment or systems.

awareness programs were in place. We destroyed all usernames and passwords collected during the testing.

We engaged the Security Research Institute at Edith Cowan University to assist us with the audit and acknowledge our long-standing relationship with them. Publicly available tools and resources (such as LG entity websites, professional networking sites and news articles) were used to map the LG entities' cyber footprints and to identify staff email addresses and potential weaknesses in the LG entities' systems and networks.

Conclusion

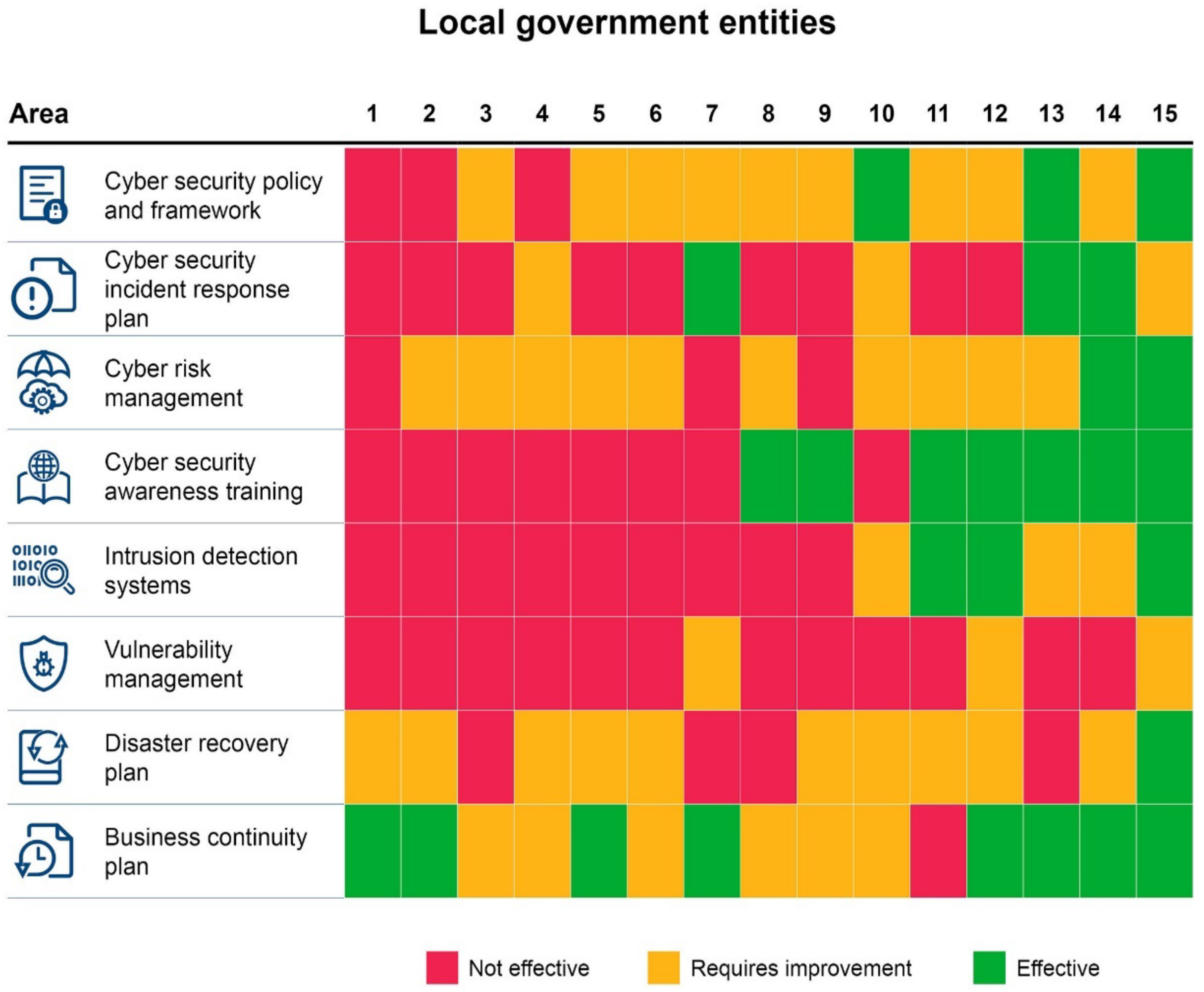
LG entities need to improve their management of cyber risks and response to cyber threats. Most did not have current and complete cyber security policies and processes to help them manage the risks and effectively respond.

Despite LG entities providing cyber security awareness training for employees, staff at 8 of the 15 audited LG entities accessed links and, in some cases, provided their credentials (username and password) in response to our test phishing emails. Technical controls to prevent phishing emails, coupled with focussed training to remind staff of their obligations and cyber security risks, would help LG entities manage these risks.

LG entities did not have appropriate mechanisms to detect and respond to cyber security incidents and their systems and networks were vulnerable because of out-of-date software. Nine of the 15 audited LG entities did not detect or respond to our simulated cyber-attacks, and those that did still needed to improve their processes.

What we found

Figure 1 summaries our findings for the 15 audited LG entities. We have anonymised the findings so as not to expose those LG entities with weaknesses to cyber-criminals.



Local government entities

Area	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Cyber security policy and framework	🟥	🟥	🟨	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟨	🟩	🟨	🟩
Cyber security incident response plan	🟥	🟥	🟥	🟨	🟥	🟥	🟩	🟥	🟥	🟨	🟥	🟥	🟩	🟩	🟨
Cyber risk management	🟥	🟨	🟨	🟨	🟨	🟨	🟥	🟨	🟥	🟨	🟨	🟨	🟨	🟩	🟩
Cyber security awareness training	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩
Intrusion detection systems	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟩	🟩	🟨	🟨	🟩
Vulnerability management	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟥	🟥	🟥	🟨	🟥	🟥	🟨
Disaster recovery plan	🟨	🟨	🟥	🟨	🟨	🟨	🟥	🟥	🟨	🟨	🟨	🟨	🟥	🟨	🟩
Business continuity plan	🟩	🟩	🟨	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟥	🟩	🟩	🟩	🟩

🟥 Not effective 🟨 Requires improvement 🟩 Effective

Source: OAG

Figure 1: LG entity findings for key audit areas

Most LG entities did not have effective cyber security policies and procedures

Only 3 LG entities had adequate cyber security policies to govern and manage cyber security. Nine LG entities had policies that were out of date or did not cover important areas. The remaining 3 LG entities did not have a policy or framework. Without policies that clearly outline the principles and expectations of systems and employees, entities are at higher risk of compromise by cyber threats. This may result in financial loss, reputational damage or disruption to the delivery of important services to their communities.

LG entities need to support their cyber security policies with good practice procedures and controls. Good practice principles, such as the *Australian Government Information Security Manual*[5] and the Australian Cyber Security Centre's Essential Eight[6] mitigation strategies, provide useful guidance on how to protect systems and information from cyber threats. LG

[5] https://www.cyber.gov.au/acsc/view-all-content/ism (current as at 22/11/2021)

[6] https://www.cyber.gov.au/acsc/view-all-content/essential-eight (current as at 22/11/2021)

entities should give regard to these principles when implementing their cyber security policies.

We identified important areas that were not defined in most of the audited LG entities' policies or procedures. These included:

- **cyber security responsibilities** to manage cyber security risks had not been clearly assigned
- **end-point security** requirements to secure devices were not established (for example anti-malware controls, hardening, and encryption)
- **access management** requirements and responsibilities to request, grant, review, and revoke access to key systems had not been defined
- **authentication requirements** to access systems had not been established or minimum requirements had not been enforced (for example password composition and multifactor authentication)
- **application controls** to ensure that only allowed applications can run on devices had not been established
- **information and system backups** to regularly backup systems and information had not been defined
- **system monitoring** to detect and respond to malicious behaviour and system events had not been established.

Most LG entities did not manage all their cyber risks

Only 2 LG entities had identified all their cyber risks, and 3 had not identified any. Ten LG entities had considered some, but not all, of their cyber risks. If LG entities are not aware of their cyber risks, they cannot mitigate them. This exposes them to higher risk of compromise which may adversely impact their business plans and objectives.

Risks that LG entities did not consider include:

- malware and ransomware
- data breaches
- unauthorised access to systems or networks (external hack)
- theft of IT devices
- third-party supply chain / cloud risks.

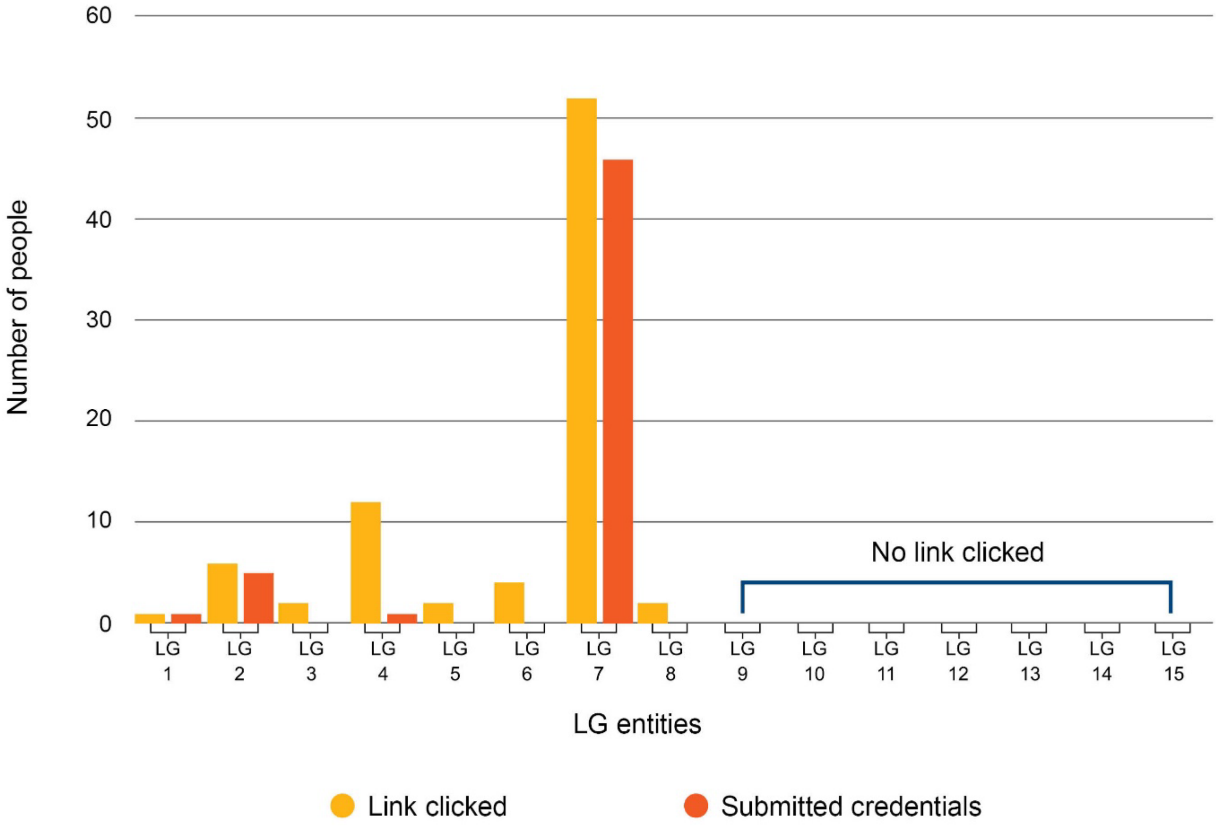
Case study 1: LG entities had not identified the risks of email compromise from external breaches

Staff might use their work email address and the same or a similar password to sign up for personal or work-related third-party services (such as Dropbox and LinkedIn). We found that all of the audited LG entities had one or more of their emails listed in historic external breaches. Ten LG entities did not have a process in place to know if their email addresses or domain appeared in external breaches and the risks this posed to them. Cybercriminals could use information from these beaches to gain unauthorised access to LG email accounts to commit fraud. Without clearly defined expectations of staff and processes to know if such incidents occur, LG entities are at higher risk of cyber security breaches.

In one publicly reported private sector example, an Australian organisation suffered reputational and financial damage after cybercriminals gained unauthorised access to the organisation's email account and used the access to send false invoices. While most of the $8.7 million paid by the organisation to the cybercriminals was recovered, the organisation declared bankruptcy after it could not sustain operations due to the reputational damage from this cyber breach.[7]

Most LG entities conducted cyber security awareness training, but remain at significant risk

Awareness programs alone will not protect LG entities from cyber-attacks. We found staff from 8 LG entities (7 with training in place, 1 without) clicked on the links in our test phishing emails and, in some cases, submitted their credentials (username and password) (Figure 2). This type of information can be used to compromise key systems or deliver malware to maintain long-term access into entity networks.



Source: OAG

Figure 2: Number of people who responded to test phishing emails at each LG entity

Cyber security awareness programs should be ongoing and focus on current trends (for example soft skills to counter cyber-attacks that exploit human behaviour). Further, if awareness programs are overly technical, individuals will not understand the cyber risks posed to their entity and their personal responsibilities. Entity systems and information can be compromised by one individual clicking on one malicious link.

[7] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (current as at 22/11/2021)

In 2020-21, phishing attacks was 1 of the highest categories for cyber incidents.[8] Our black box test exercise found LG entities were at significant risk from these attacks.

Case study 2: Forwarded email increased the number of people who accessed the link and gave their credentials

At 1 audited entity, 4 staff clicked on the link in our test phishing email and 2 submitted their credentials. One of the 4 staff forwarded our test email to other staff and external contacts who were not part of our initial target list. This resulted in an additional:

- 29 staff clicking the link and providing their credentials
- 15 external contacts clicking the link and providing their credentials
- 4 who clicked the link but did not provide any credentials.

This case study shows that people generally trust and are more likely to respond to emails from known contacts. Regular and up-to-date cyber security awareness training and controls to detect and prevent phishing emails are important to combat such attacks.

LG entities did not address vulnerabilities in a timely manner

We found that only 3 audited LG entities had a process to manage vulnerabilities[9] and none of these were fully effective. We expected LG entities to have timely processes to address vulnerabilities.

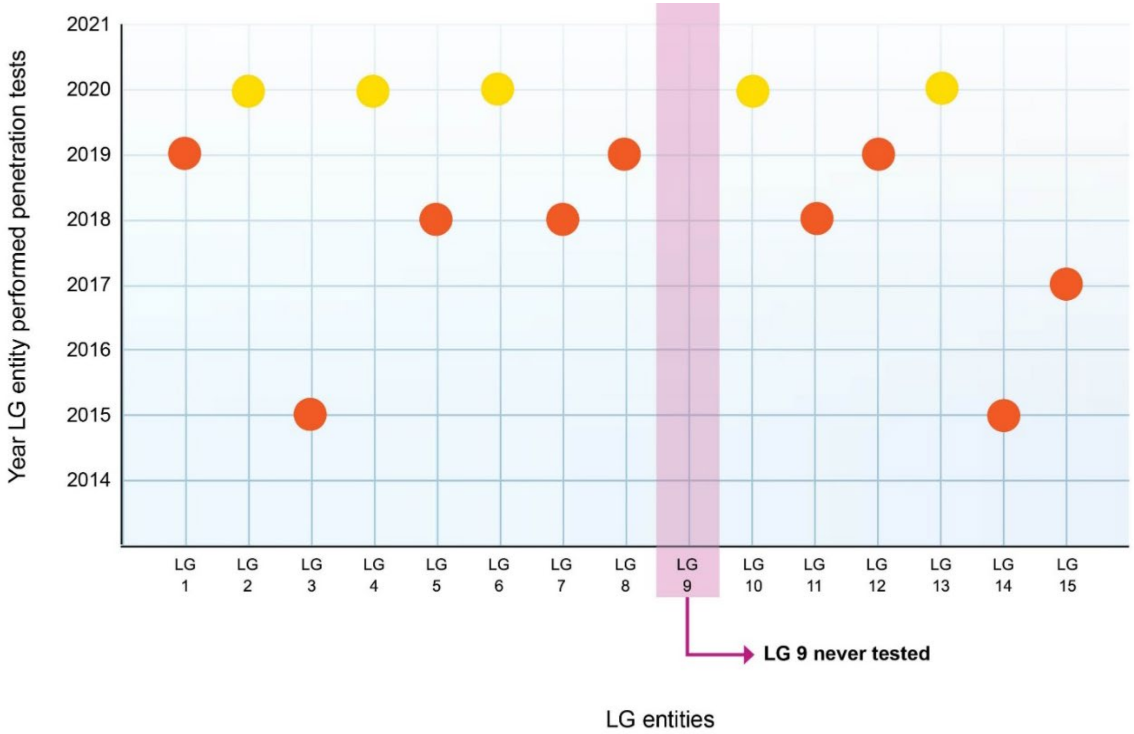
State sponsored actors and cybercriminals exploit vulnerabilities to disrupt and compromise systems. For example, using specially crafted malware that bypasses basic security controls. The Australian Cyber Security Centre observed that in some cases, known vulnerabilities were exploited within hours after they are made public.[10] Vulnerabilities can be due to things such as flawed, misconfigured and unpatched software, misconfigured devices, and poor security controls.

Only 5 audited LG entities had recently tested (penetration tests) the effectiveness of their security controls which protect them from cyber-attacks. Two LG entities had not conducted tests since 2015 (Figure 3) and 1 had never tested. LG entities are at higher risk of compromise if they do not identify and address weaknesses.

[8] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (current as at 22/11/2021)

[9] Vulnerabilities are weaknesses that can be exploited by cybercriminals to compromise systems and information.

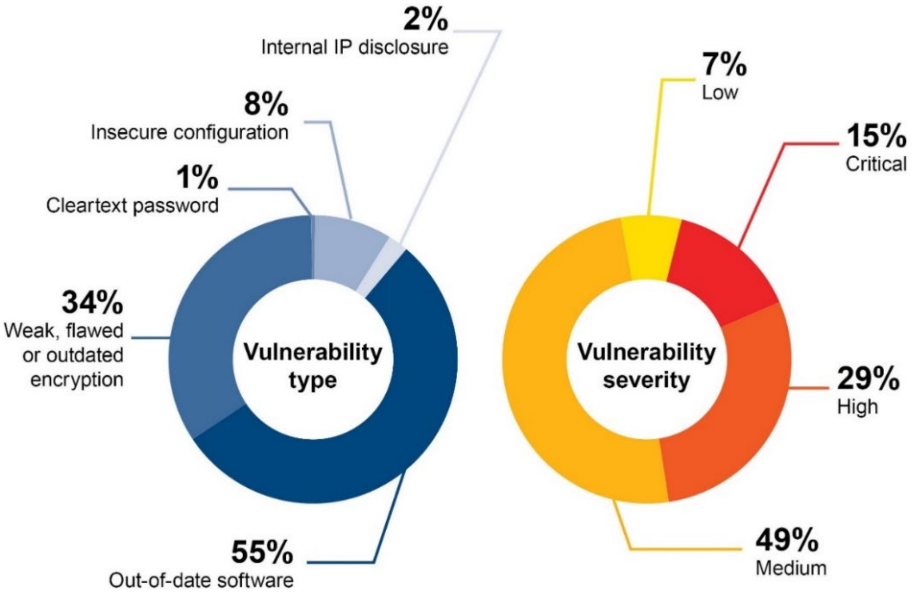
[10] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 (current as at 22/11/2021)



Source: OAG

Figure 3: Entities' most recent network penetration tests

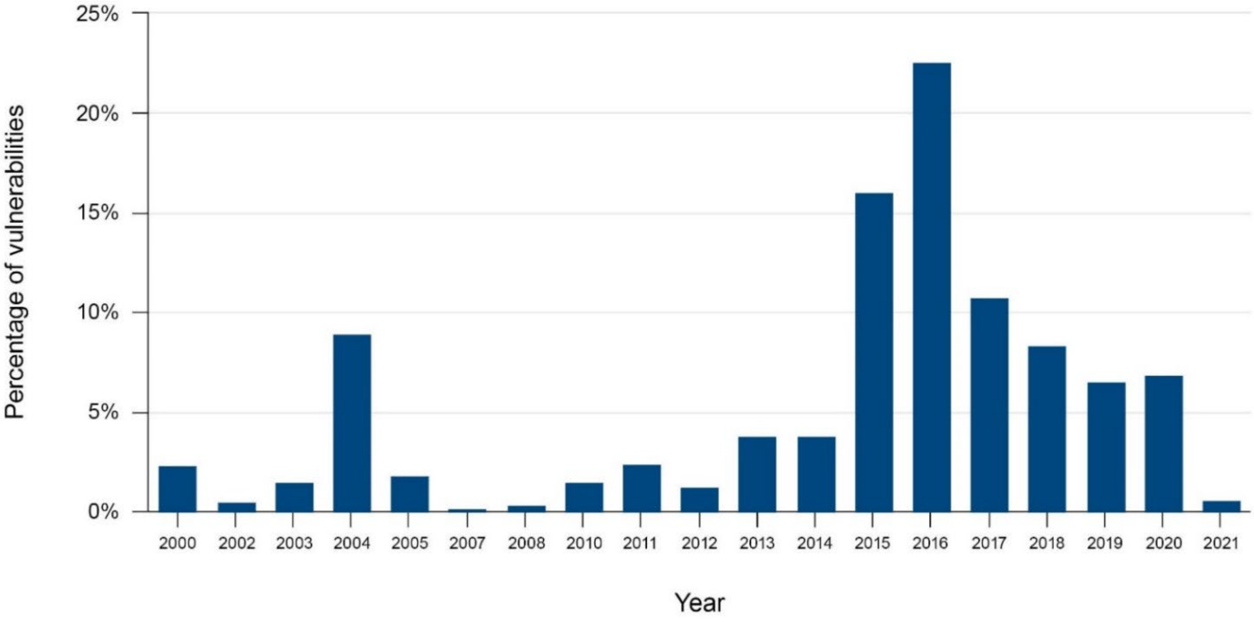
We tested the audited LG entities' publicly accessible IT infrastructure and found vulnerabilities of varying types, severity and age. The vulnerabilities included disclosure of technical information, out-of-date software, flawed or weak encryption, insecure software configuration and passwords sent in cleartext over the internet. Out-of-date software accounted for most of the vulnerabilities identified (Figure 4). Forty four percent of vulnerabilities were of critical and high severity, with a further 49% of medium severity. Known critical and high severity vulnerabilities are generally easy to exploit and expose LG entities to increased risk of compromise.



Source: OAG

Figure 4: Type and severity of vulnerabilities

Most vulnerabilities were older than 12 months, with some dating back over 15 years (Figure 6). LG entities need a process to address vulnerabilities in a timely manner if they are to reduce the risk of disruption to services and systems from cyber-attacks.



Source: OAG

Figure 6: Age of vulnerabilities

The following case study shows why it is important for LG entities to identify and fix vulnerabilities in a timely manner.

Case study 3: Out-of-date software and a weak password leaves LG entity websites vulnerable

We found an audited metropolitan LG entity with an active legacy website that it did not know still existed. We identified several vulnerabilities affecting the website including:

- out-of-date software components
- disclosure of server configuration details.

Using the above vulnerabilities, we bypassed authentication to access this legacy site. The site contained historic information on application approvals (such as business names, liquor licence application data, business permit application data, and resident names) and server logs which disclosed further technical information.

This entity also had an old library website which was vulnerable due to a very weak password. We guessed the password and accessed protected parts of the old library website. This access could be used to change the website.

A cybercriminal could post offensive materials on these websites to cause reputational damage to the entity or access sensitive information for inappropriate use.

The LG entity informed us of its intent to decommission the legacy sites.

LG entities need to improve their response and recovery strategies

To effectively respond to cyber-attacks, we expected LG entities to have:

- **cyber security incident response plan** – to assess and respond to cyber security related incidents
- **disaster recovery plan** – to recover key systems from any disaster situation
- **business continuity plan** – to continue the delivery of key services in a disaster scenario and resume normal operations
- **intrusion detection systems** – to detect, alert and prevent cyber intrusions.

Twelve LG entities did not have an effective incident response plan to adequately respond, report and escalate cyber security incidents in a timely manner. This could impact LG entities' key IT systems and services and affect business operations. Most LG entities had a business continuity plan and disaster recovery plan, although some needed to be updated and improved. Testing these plans is also vital to familiarise staff with them and implement improvements as required.

We used basic open-source tools to simulate cyber-attacks on the 15 audited LG entities to test their response strategies. Only 3 LG entities had their systems configured to detect and block our simulated attacks in a timely manner. These LG entities demonstrated an effective response to cyber intrusions to protect their systems and information.

It was concerning that 9 LG entities did not detect nor respond to our simulations, and 3 LG entities took up to 14 days to detect the simulations, and only did so after the simulation intensity increased significantly. These 12 LG entities had intrusion detection systems, but processes were not in place to analyse information generated by the systems in a timely manner. Without these processes, LG entities may not effectively respond to cyber intrusions in time to protect their systems and information.

Recommendations

All LG entities should adopt:

1. cyber security policies aligned to relevant cyber security frameworks and standards, such as the *Australian Government Information Security Manual*
2. processes to identify, understand, and address relevant cyber security risks
3. relevant controls from the Australian Cyber Security Centre's Essential Eight mitigation strategies
4. ongoing awareness raising programs to education staff on cyber security risks
5. technical controls to detect and prevent phishing emails
6. processes to identify and address vulnerabilities affecting their internal and external IT infrastructure
7. appropriate cyber security incident response strategies covering:
    a. cyber security incident response plan
    b. business continuity plan
    c. disaster recovery plan
    d. technical controls to detect, alert and prevent cyber intrusions.

Response from LG entities

All 15 LG entities reviewed during the audit generally accepted the recommendations.

Appendix 1 – Better practice principles to manage cyber security risks

The following table outlines guiding principles for entities to consider when managing their cyber security risks. This is not intended to be an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre (ACSC). [11]

Guiding principles	
Understand cyber security risks	Identify and assess cyber risks to systems and information and implement appropriate plans to address them.
Develop a cyber security policy	Develop and implement a cyber security policy that aligns with better practice frameworks such as the Australian Information Security Manual.
Regularly test control effectiveness	Regularly test the effectiveness of security controls which protect against cyber-attacks and address vulnerabilities in a timely manner.
Develop response plans	Develop incident response, business continuity and disaster recovery plans to manage and recover from cyber security incidents. Test these plans regularly.
Secure emails	Secure emails with controls such as sender policy framework and domain-based message authentication. Implement controls to detect suspicious emails and attachments (e.g. phishing).
Educate staff	Develop awareness programs that are not overly technical to educate staff on cyber and information security risks.
Intrusion detection	Implement controls to identify and block malicious intrusions.
Protect endpoints	Use application control and modern anti-malware software to protect endpoints from threats, including mobile devices.
Use encryption	Use encryption to protect data from theft. This should apply to data at rest and in movement and include mobile devices.
Limit administrative privileges	Administrators should have separate accounts to perform privileged tasks. These should be regularly reviewed to ensure only appropriate staff have these privileges and that they still require it.
Apply software updates	Implement processes to receive alerts when patches are released by vendors and apply them to applications and operating system software in a timely manner.
Use passphrases	Develop and implement passphrase policies to manage authentication on supported systems.
Multi-factor authentication	Implement multi-factor authentication to protect systems from unauthorised access.
Backup systems and information	Regularly backup and test restoration of systems and information. Protect the integrity of backups in case the primary dataset is compromised or infected with malware.
Harden user applications	Disable or remove unwanted applications and features such as unnecessary browser plugins and software frameworks.
Cyber security monitoring/ situational awareness	Use event data to know what is occurring on your network. Develop processes to receive alerts if accounts, passwords or vulnerabilities related to your entity are disclosed through breaches.
Collaborate	Liaise with key cyber security entities such as the ACSC and their Joint Cyber Security Centre.

Source: OAG

[11] https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents (current as at 22/11/2021)

Auditor General’s 2021-22 reports

Number	Title	Date tabled
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

OAG
Office of the Auditor General
Serving the Public Interest

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for
Western Australia