Information Systems Audit Report 2018

Summary

Report 1: August 2018-19

Password Management in the WA State Government

Introduction

Western Australian government agencies collect and store a significant amount of sensitive and confidential information. The public rightly expects agencies to protect this information from unauthorised access. Effective management and use of passwords remains a vital part of information security. However, since 2004 our information systems audits have consistently raised issues around agency access controls, particularly passwords.

The objective of this audit was to determine if selected government agencies are using good practices to manage network passwords, to protect the information they hold.

Conclusion

Over one quarter of the enabled network accounts we looked at had weak passwords at the time of audit. In a number of instances these accounts are used to access critical agency systems and information via remote access without any additional controls.

Generally, agencies lacked technical controls to enforce good passwords across networks, applications and databases, and did not have guidance about good practice for password management.

Background

Agencies have a diverse range of users, applications and services with different purposes and security requirements. These require different types of accounts or identities to access information from inside and outside agencies. For example:

- Employees: Normal user accounts for staff to perform day-to-day tasks
- Partners: contractors and vendor support staff
- Privilege Accounts: Individuals with high level administrative privileges such as system, network and database administrators
- Shared and Generic Accounts: Default accounts and vendor accounts that are not specific to an individual and where passwords are shared with other users
- Services and Applications: Accounts used by operating system services and applications such as web servers, email services and backup accounts.

Passwords are still the main control agencies use to protect information systems and are an important security mechanism for all account types. Good password management practices combine people, process and technology to secure the use and management of passwords. Creating complex, hard to guess passwords requires at least 3 of the following categories:

- uppercase
- lowercase
- digits (0 through 9)
- non-alphanumeric characters (e.g. !, $).

However, passwords that meet complexity requirements, may still be considered weak if they use common variations of words or keyboard patterns or are included in publicly available password dictionaries.

The importance of password security is well known. The July 2018 *Notifiable Data Breaches Quarterly Statistics Report*[1] stated that 59% of data breaches involved malicious attacks, with most the result of compromised credentials. Phishing and brute force accounted for 43% of the attacks. Another global report[2] linked 81% of hacking-related breaches to stolen or weak passwords. Globally it is estimated that each data breach cost an average of US$3.62m[3].

What we did

As part of our annual information systems audits, we assessed 17 agencies' processes and controls in place to manage passwords and privileged accounts. We processed about 520,000 enabled and disabled accounts across agencies' Active Directory (AD) environments by collecting the AD information using encrypted USBs. We analysed and disposed of the information in a secure offline environment. In performing this work, we:

- assessed encrypted passwords from each agency's AD environments. We also assessed old disabled accounts to understand password composition trends over time. Where possible, we used data from the AD to determine the account purpose and level of privilege for each of the accounts
- used a password cracking method known as Dictionary Attack and a list of well-known or commonly used passwords such as 'Password1' and 'Welcome123'. We compiled the list from publicly available password dictionaries used for penetration testing assessments. Weak passwords not on our list were not identified as part of our testing
- reviewed agency policies and security awareness training
- provided agencies with information so they can implement strong passwords for identified weak accounts.

[1] https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018.pdf
[2] https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf
[3] https://www.ibm.com/security/data-breach

Application Controls Audits

Introduction

Applications are software programs that facilitate an organisation's key business processes including finance, human resources, case management, licensing and billing. Applications also facilitate specialist functions that are unique and essential to individual entities.

Each year we review a selection of important applications that agencies rely on to deliver services. We focus on the key controls that ensure data is completely and accurately captured, processed and maintained. Failings or weaknesses in these controls have the potential to affect other organisations and the public. Impacts range from delays in service and loss of information, to possible fraudulent activity and financial loss.

Audit focus and scope

We reviewed key business applications at 5 agencies. Each application is important to the operations of the agency and may affect stakeholders, including the public, if the application and related processes are not managed appropriately.

The 5 agency applications we reviewed were:

1. **Patient Medical Record System** – Department of Health
2. **Tenancy Bonds Management System** – Department of Mines, Industry Regulation and Safety
3. **First Home Owner Grant Online System** – Office of State Revenue
4. **Election Management System WA** – Western Australian Electoral Commission
5. **Keysmart System** – Keystart Housing Scheme Trust

Our application reviews look at the systematic processing and handling of data in the following categories:

1. **Policies and procedures** – are appropriate and support reliable processing of information
2. **Security of sensitive information** – controls exist to ensure integrity, confidentiality and availability of information at all times
3. **Data input** – information entered is accurate, complete and authorised
4. **Backup and recovery** – is appropriate and in place in the event of a disaster
5. **Data output** – online or hard copy reports are accurate and complete
6. **Data processing** – information is processed as intended, in an acceptable time
7. **Segregation of duties** – no staff perform or can perform incompatible duties
8. **Audit trail** – controls over transaction logs ensure history is accurate and complete
9. **Masterfile maintenance, interface controls, data preparation** – controls over data preparation, collection and processing of source documents ensure information is accurate, complete and timely before the data reaches the application.

Our testing of the above categories of controls is a point in time assessment. It is based on a sample of key controls and processes that are designed to obtain reasonable assurance about whether an application works as intended and that the information it contains and reports is reliable, accessible and secured. Our testing of some of those controls may highlight weaknesses in their design or implementation that increases the risk that an application's

information may be susceptible to compromise. However, we do not design our tests to specifically determine whether information has been compromised.

Summary

All 5 applications had control weaknesses with most related to poor information security and policies and procedures. We also found issues with controls that aim to ensure the applications function efficiently, effectively and remain available. We reported 49 findings across the 5 applications with 9 of these rated as significant, 29 moderate and 11 minor.

Correcting most of the issues we raised is relatively simple and inexpensive. Figure 1 shows the findings for each of the areas and Figure 2 shows the findings for each of the 5 applications reviewed.

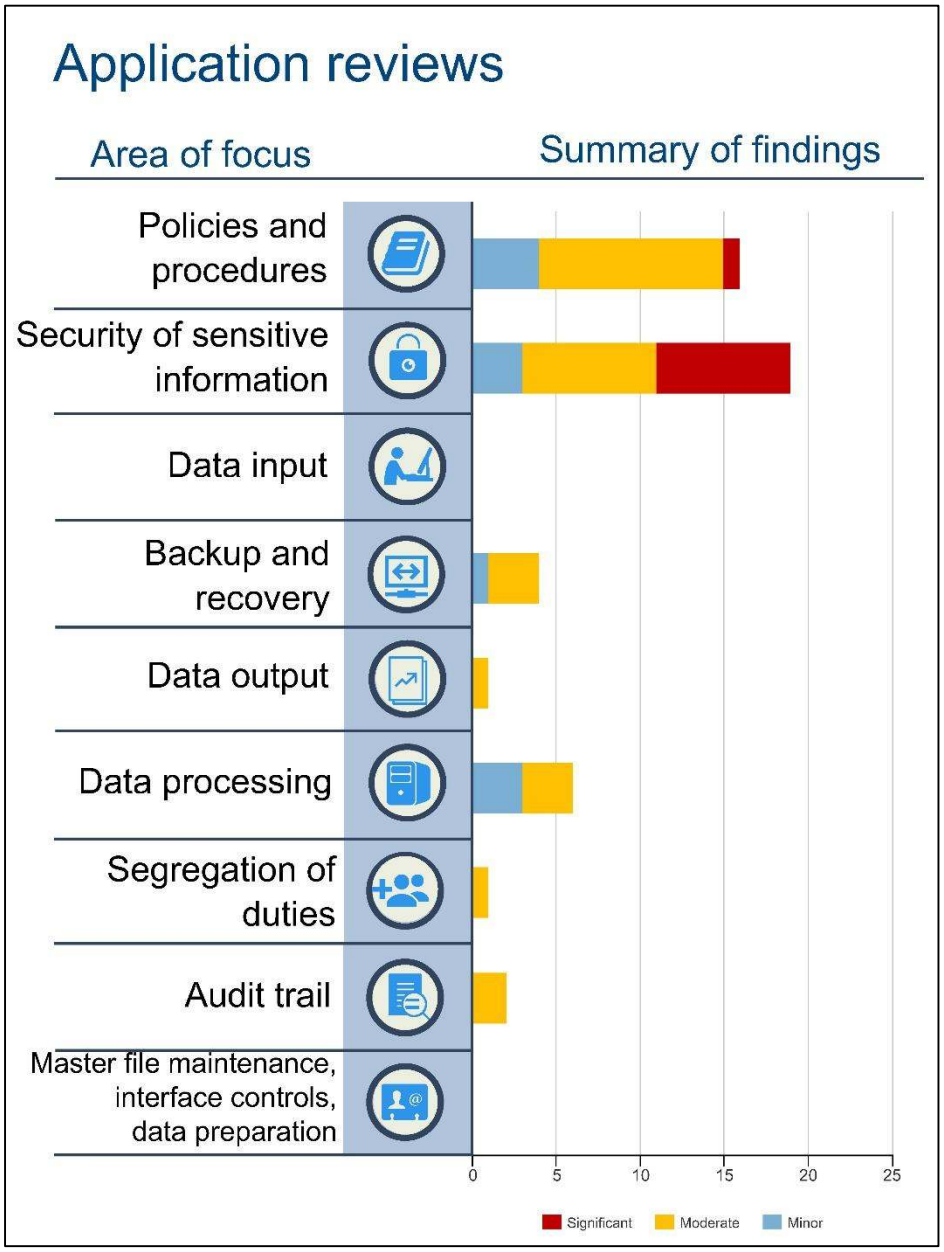

Figure 1: Application reviews

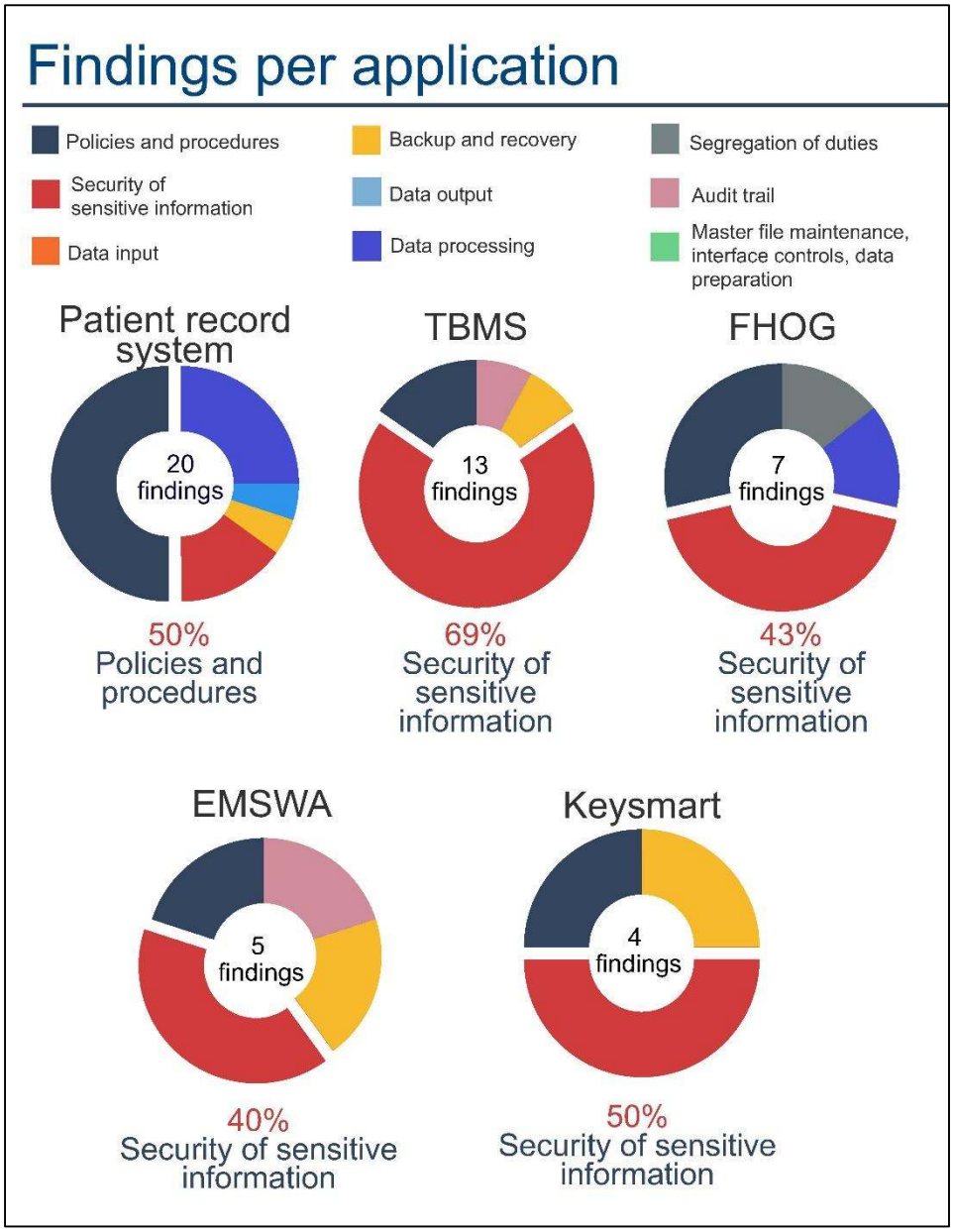

Figure 2: Findings per application

General Computer Controls and Capability Assessments

Introduction

The objective of our general computer controls (GCC) audits is to determine whether computer controls effectively support the confidentiality, integrity, and availability of information systems. General computer controls include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. In 2017 we focused on the following control categories:

- information security
- business continuity
- management of IT risks
- IT operations
- change control
- physical security.

Conclusion

We reported 539 general computer controls issues to the 47 agencies audited in 2017 compared with 441 issues at 46 agencies in 2016. This increase is, in part, due to a more detailed assessment into all general control categories in 2017.

There was an increase in the number of agencies assessed as having mature general computer control environments across all 6 categories of our assessment. Ten agencies met our expectations for managing their computer environments effectively, compared with only 6 in 2016.

While system change controls and physical security are managed effectively by most agencies, 2 of the categories, information security and business continuity, have shown little improvement in the last 10 years. The majority of issues we have identified can be easily addressed with better password management and ensuring processes to recover data and operations in the event of an incident are kept updated.

By not prioritising the security and continuity of information systems, agencies risk disruption to the delivery of vital services to the community and compromise the confidentiality and integrity of the information they hold.

Background

We use the results of our GCC work to inform our capability assessments of agencies. Capability maturity models are a way of assessing how well developed and capable the established IT controls are. The models provide a benchmark for agency performance and a means for comparing results from year to year.

The models we developed use accepted industry good practice as the basis for assessment. Our assessment of the appropriate maturity level for an agency's general computer controls is influenced by various factors. These include: the business objectives of the agency; the level of dependence on IT; the technological sophistication of their computer systems; and the value of information managed by the agency.

Audit focus and scope

We conducted GCC audits at 47 agencies. This is the tenth year we have assessed agencies against globally recognised good practice.

We provided 40 of the 47 agencies with capability assessment documentation and asked them to complete and return the forms at the end of the audit. We then met with each of the

agencies to compare their assessment and ours, which was based on the results of our GCC audits. Seven agencies, whose GCC audits were outsourced, were not included in the capability assessment.

We use a 0-5 scale rating[4] to evaluate each agency's capability maturity level in each of the GCC audit focus areas. The models provide a baseline for comparing results for agencies from year to year. We have included specific case studies where information security weaknesses potentially compromise agencies' systems.

0 Non-existent	Management processes are not applied at all. Complete lack of any recognisable processes.
1 Initial/ad hoc	Processes are ad hoc and overall approach to management is disorganised.
2 Repeatable but intuitive	Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.
3 Defined	Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated, however it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 Managed and measurable	Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimised	Good practices are followed and automated. Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the agency quick to adapt.

Table 1: Rating criteria

[4] The information within this maturity model assessment is based on the criteria defined within the Control Objectives for Information and related Technology (COBIT) manual.