Focus On

Information Technology Security

CANADIAN AUDIT & ACCOUNTABILITY FOUNDATION

A PRODUCT OF AUDIT NEWS

About the Canadian Audit and Accountability Foundation

The Canadian Audit and Accountability Foundation is a premier Canadian research and education foundation. Our mission is to strengthen public sector performance audit, oversight, and accountability in Canada and abroad. We build capacity in legislative audit offices, oversight bodies, and departments and crown corporations by developing and delivering:

- Training workshops and learning opportunities;
- Methodology, guidance, and toolkits;
- Applied and advanced research;
- Information sharing events and community building initiatives.

Visit us at www.caaf-fcar.ca for more information about our products and services.

Focus On Information Technology Security

© 2018 Canadian Audit and Accountability Foundation

All rights reserved. No part of this publication, or its companion products, may be reproduced by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

Published by:

Canadian Audit and Accountability Foundation
100-1505 Laperriere Avenue
Ottawa, Ontario CANADA
K1Z 7T1

Tel: 613-241-6713
info@caaf-fcar.ca
www.caaf-fcar.ca

ISBN: 978-1-7752844-0-6

This publication is available in French under the title:
Pleins feux sur la sécurité des technologies de l'information

Table of Contents

Introduction

The Audit News *Focus On* Series

The Audit News *Focus On* series is intended to help performance auditors complete audit planning and examination work more rapidly.

The series is designed to be useful for:

- auditors preparing a strategic audit plan,
- auditors working on the planning phase of a new performance audit, and
- auditor managers with ongoing responsibilities for a specific topic or entity.

Each *Focus On* issue covers one broad topic that should be of interest to most performance auditors, whether they work at the municipal, provincial, or federal level.

Each issue includes:

- a short introduction to the topic and why it is important
- a list of relevant audits and guidance material on the topic that have been released in the previous five years and compiled in the Audit News Database
- a summary of each relevant audit selected that includes information on audit objective(s), criteria, findings, and recommendations
- an analysis of the main audit areas covered by relevant audits in the past five years
- web links to full audit reports and guidance documents referenced in the issue

To help auditors in their planning and examination work, we have included a glossary of information technology terms used in this issue and in the audits we selected for inclusion.

We plan to release more *Focus On* issues. Please contact us at info@caaf-fcar.ca if you have suggestions for future topics.

Back to Table of Contents

Information Technology Security—Why It's Important

Information technologies are ubiquitous in the 21st century. Smart phones, tablets, and various other connected devices have, in only a few years, become fully integrated in our daily lives. The pace of technological innovation is steadily accelerating, with futuristic-sounding ideas, like self-driving cars, being set to soon become a reality.

While all these new technologies have brought citizens of all nations important benefits and opportunities, they have also introduced new risks that need to be carefully managed. Computer viruses, ransomware, phishing, hacking, and identity theft are all examples of information technologies being used for wrongful purposes, often with disastrous and costly results. Rarely a month goes by without the news media reporting yet another large corporation being hacked and the private information of thousands, sometimes millions, of individuals being stolen by cyber pirates (be they thrill-seeking teenagers, "hacktivists," perpetrators of organized crime, terrorists, or hostile state actors).

The wrongful use of information technologies can have consequences far beyond the theft of private information. Public sector organizations are also at risk. In recent times, for example, cyber pirates have successfully stolen more than 20 million personnel records at the United States Office of Personnel Management and deleted all the data in Saudi Arabia's national oil company's IT systems. In the United Kingdom, they also took many hospital IT systems hostage through the use of ransomware, forcing some hospitals to cancel non-urgent appointments.

Furthermore, because public industrial and transport infrastructure are now increasingly connected to corporate networks and the Internet, they have become susceptible to cyber attacks that can cause physical damage and disrupt important services. For example, in recent years, hackers have managed to temporarily shut down electricity generation in Ukraine and also damaged a steel mill in Germany and nuclear program equipment in Iran.

All connected assets, from smart phones to self-driving cars to industrial control systems, are, to some extent, at risk of being hacked. And, as time passes, the number and types of connected devices increase rapidly, as does the number of hackers and their skills at finding weaknesses in IT systems.

In this environment, public sector organizations must remain hyper-vigilant. They must implement the latest good practices in IT risk management to protect their IT assets from unauthorized access and to prevent the use, disclosure, disruption, modification, review, and destruction of the information they contain.

Only by effectively managing their IT security risks will public sector organizations be able to:

- protect the confidentiality, integrity, and availability of the information they possess;
- protect key public infrastructure, such as electricity production installations and public transit systems, from cyber attacks; and
- ensure business continuity and the availability of services to citizens.

Internal and legislative auditors can support public sector organizations to achieve these goals by providing independent assurance about whether IT security risks are well managed and by making recommendations for improvements where needed.

Back to Table of Contents

Overview of 2013–2017 Information Technology Security Audits

Using the Audit News Database, we searched for IT security audits conducted since 2013. We found more than 30 audits prepared by 17 audit offices. For this *Focus On* issue, we selected 16 of these audits for further analysis.

See list of selected IT security audits

We also noted the availability of two guidance documents on IT controls published by the Victorian Auditor-General's Office and by the INTOSAI Development Initiative (IDI), respectively:

- Information and Communications Technology Controls Guide (2016)
- IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

We analyzed the scope of the selected audits and listed all the sub-topics covered in the audits. We then mapped the contents of each audit against this list of sub-topics. The results of this analysis are presented in the Main Audit Areas section.

In addition, definitions of selected technical terms used in these reports and that auditors may encounter during IT audits can be found in the Glossary at the end of this document.

Because of security concerns, it is sometimes necessary for auditors general not to publicly disclose the findings and recommendations of their IT security audits or to disclose only aggregated audit findings. For this reason, this *Focus On* issue cannot present the full range of IT security audit findings and recommendations. The information presented in this issue was gathered from publicly available documents.

Back to Table of Contents

List of Selected Information Technology Security Audits

#	Audit Office	**Report Title** (click on title to access audit summary)	Publication Date
1	Office of the Auditor General—City of Québec	Information Security Governance	2017
2	Office of the Auditor General of British Columbia	An Independent Audit of the Regional Transportation Management Centre's Cybersecurity Controls	2017
3	Office of the Auditor General of Ontario	Independent Electricity System Operator—Market Oversight and Cybersecurity	2017
4	Office of the Auditor General of Alberta	IT Security for Industrial Control Systems in Alberta's Oil and Gas Industry	2016
5	Victorian Auditor-General's Office	Security of Critical Infrastructure Control Systems for Trains	2016
6	Provincial Auditor of Saskatchewan	Central Services—Web Application Security Requirements	2016
7	Provincial Auditor of Saskatchewan	Central Services—Data Centre Security	2016
8	Office of the Auditor General Western Australia	Malware in the WA State Government	2016
9	Auditor-General's Department, South Australia	Security Management of Information Systems	2016
10	Provincial Auditor of Saskatchewan	SaskPower—Managing the Risk of Cyber Incidents	2015
11	Office of the Auditor General of Manitoba	Manitoba Hydro—Managing Cyber Security Risk Related to Industrial Control Systems	2014

#	Audit Office	**Report Title** (click on title to access audit summary)	Publication Date
12	Office of the Auditor General of the City of Montréal	Security of Wireless Networks	2014
13	Australian National Audit Office	Cyber Attacks: Securing Agencies' ICT Systems	2014
14	Victorian Auditor-General's Office	WoVG Information Security Management Framework	2013
15	Office of the Auditor General of Manitoba	Information Technology (IT) Security Management Practices	2013
16	Office of the Auditor General of British Columbia	Securing the JUSTIN System: Access and Security Audit at the Ministry of Justice	2013

Back to Table of Contents

Main Audit Areas

As part of our review of the selected audits, we identified about 20 audit areas (or sub-topics) that can fall under the scope of a performance audit on IT security. We selected the 10 sub-topics that had received the most emphasis (see text box) and mapped the content of each audit against these sub-topics. The result of this analysis is presented in **Table 1**. For each audit in the table, there is a link to the audit summary we prepared. Each summary in turn includes a link to the published audit report.

Sub-topics identified in selected audits (alphabetical order)

- Application whitelisting
- Business continuity
- Governance
- Logical access
- Malware
- Networks
- Patches
- Security awareness
- Vulnerability assessments
- Web applications

The 10 selected sub-topics are all relevant for auditors interested in auditing IT security. The following information briefly explains why each sub-topic can be an important element to consider when planning an audit and mentions some specific elements to inquire about.

Application whitelisting. Application whitelisting is a control that protects against unauthorized applications on a system. Whitelisting can be an effective mechanism to prevent IT systems from being compromised by the execution of malicious code.

To be effective, whitelisting requires (1) a policy that defines what types of application users are allowed to run on their devices as part of their duties, (2) a detailed list of approved applications, and (3) technical implementation that meets the policy's intent.

Business continuity. Cyber attacks and data breaches can significantly disrupt an organization and even prevent it from providing key services to the public. A cyber attack can result in lost data, compromised personal or financial information, unplanned downtime, and other challenges.

To mitigate the consequences of a cyber attack, organizations should integrate IT security measures in their business continuity plan. This plan should include, among other things, information on data backup and recovery processes.

Table 1 – Audit Scope for Each of the 16 Selected Audits

	Application Whitelisting	Business Continuity	Governance	Logical Access	Malware	Networks	Patches	Security Awareness	Vulnerability Assessments	Web Applications
1. OAG – City of Québec		✓	✓					✓	✓	
2. OAG – British Columbia				✓					✓	
3. OAG – Ontario			✓	✓					✓	
4. OAG – Alberta			✓							
5. Victorian Auditor-General's Office		✓	✓						✓	
6. Provincial Auditor of Saskatchewan										✓
7. Provincial Auditor of Saskatchewan		✓	✓	✓		✓				
8. OAG – Western Australia					✓			✓		
9. Auditor-General's Department, South Australia	✓			✓			✓			
10. Provincial Auditor of Saskatchewan		✓	✓	✓					✓	
11. OAG – Manitoba			✓					✓		
12. OAG – City of Montréal						✓				
13. Australian National Audit Office	✓		✓	✓			✓			
14. Victorian Auditor-General's Office			✓					✓		
15. OAG – Manitoba			✓					✓		
16. OAG – British Columbia			✓	✓						

Governance. IT security governance is the systems and practices by which an organization directs and controls IT security. It is essentially about:

- defining roles and responsibilities,
- establishing policies,
- providing strategic directions,
- ensuring that risks are well managed,
- reviewing performance, and
- monitoring compliance with policies and regulations.

Logical access. Public sector organizations often maintain IT systems and databases that include sensitive personal information about large numbers of citizens. In the wrong hands, this data can be used for malicious purposes. Therefore, strict controls should ensure that only authorized personnel can access this data.

Logical access safeguards (such as defined access rights and authority levels, user identification, and passwords) should be in place to prevent the unauthorized access to IT systems and databases by outsiders seeking to exploit Internet weaknesses, or by insiders seeking to misuse their trusted status.

Networks. Workers in government organizations are connected to computer networks through which they can exchange and store sensitive information. If not adequately protected, these networks can be breached and the information they contained accessed by unauthorized users.

To prevent such breaches, proper network configurations should be maintained on all wired and wireless devices that can access the network. This includes, among other measures, using encryption software, installing and updating anti-virus software, and properly configuring firewalls, routers, and printers.

Malware. Malware (malicious software) is a harmful computer program that can steal information from a user (such as usernames and passwords, credit card numbers, or files and documents) or enable an attacker to remotely take control of a computer and access any connected network. A computer can be infected by malware by a user downloading an infected file, opening an attachment in a phishing message, or using an infected USB key.

Effective protection against malware includes up-to-date anti-virus software and operating systems, adequate monitoring of IT systems, and awareness training for public servants.

Patches. Hackers are constantly trying to find flaws in software and IT systems that will allow them to gain unauthorized access to sensitive data. As a result, IT specialists are constantly developing solutions, or patches, to identified problems in software and IT systems. Organizations that do not implement these patches on a timely basis expose their IT systems to cyber attacks.

To ensure that all required patches are implemented on a timely basis, organizations should have documented policies and processes about identifying and implementing patching requirements for workstations and servers. They should also regularly assess compliance levels with patching requirements.

Security awareness. An organization with good IT systems and a good team of IT specialists will still be at risk if its employees, who use a variety of applications each day, are not aware of internal IT policies and cannot identify behaviours that create IT risks for the organization. For this reason, providing IT security awareness training to all staff who use IT equipment should be a key element of an effective IT security strategy.

Vulnerability assessments. By having a process for ongoing detection, classification, and prioritization of vulnerabilities in its IT systems, complemented with swift actions to address priority issues, an organization can reduce the vulnerability of its IT systems and the likelihood of a successful cyber attack.

Various tools and methodologies exist to conduct assessments of networks, applications, and databases. Some of these tools are automated and can help organizations to conduct regular standardized assessments.

Web applications. Web applications are computer programs that are built into websites, and that help websites work. Public sector organizations often design Web applications that allow citizens to access specific government services. When not properly designed, Web applications can display weaknesses that can be exploited by cyber pirates to access sensitive information (such as birthdates or credit card numbers) while it is being processed by the application or being stored on a network.

To protect against such breaches, organizations should be using a multi-layered security approach that can still provide protection even if one layer is compromised. Firewalls, secure coding protocols, and logical access controls are some of the measures that can be put in place to secure Web applications.

Back to Table of Contents

Appendix 1
Audit Summaries

Focus On Series – IT Security

Audit Summary

Audit Title

Information Security Governance

Publication Date: 2017

Audit Office: Office of the Auditor General—City of Québec

Link to full report (in French):

https://www.ville.quebec.qc.ca/publications/docs_ville/VG_Rapport2016.pdf

Audited Organization

- City of Québec

Audit Objective

- Determine whether City Management is setting up the foundations required for sound governance and management of information security, and is monitoring related operations.

Audit Criteria

- The expectations of Management in terms of information security are defined and communicated to all stakeholders. In particular, these expectations deal with:
  - the security principles to be observed;
  - the roles and responsibilities of the various stakeholders;
  - the planned monitoring of the principles' observance.
- Management ensures that information assets are categorized according to their level of criticality (availability, integrity and confidentiality) and that the responsibilities of the designated holders are clearly defined and communicated.
- Management ensures that the risks associated to information security during its collection, processing, storage and destruction are inventoried and analyzed and that they are used to prioritize actions and investments in this regard.
- Management is setting up an information security management system and ensures that the required human, material and financial resources are assigned to operate it.
- Management ensures that the appropriate processes and security mechanisms are in place.
- Management ensures that an awareness and training plan is developed to build the stakeholders' awareness of information security and to equip staff who have security responsibilities with the knowledge they need.

- Management exercises the necessary monitoring for diligent management of information security, including:
    - operation of the processes in place;
    - risk coverage; and
    - efficiency of security measures.

Main Audit Findings

- City Management did not implement all the foundations necessary for appropriate management of information security and does not adequately monitor their operation. Several information security processes and mechanisms have been implemented on the basis of sectoral initiatives, but without a global perspective. Governance by the City therefore does not foster implementation of all the necessary means to ensure information security in accordance with its needs.
- Information security officers do not have the necessary foundations to fully meet the responsibilities they are assigned. They cannot lean on an integrated risk management framework.
- Because of partial management of information security risks, it is possible that major risks are not detected and not dealt with in a manner consistent with their importance.
- The audit noted problems related to the designation of responsibility holders:
    - no responsibility holder was designated for 105 of the 522 information systems (20%), including those related to 5 critical systems; and
    - the tests performed on the information systems of a business line of the City revealed a problem in 42% of cases.
- Analysis of the information security action plan for March 2014 brought to light the following shortcomings:
    - it contains a lot of general actions with no short-term priorities;
    - it does not establish links with incurred risks;
    - it does not provide for a mechanism to link planning with the various initiatives of the City that may have an impact on information security; and
    - it does not specify who is responsible for implementation of the activities, nor what efforts are planned to carry out those activities.
- Management did not put enough efforts into guiding and supporting the implementation of the security measures. Moreover, it receives little information on the nature, the operation and the efficiency of these measures.
- The main problems discovered in terms of incident management are:
    - the procedures to respond to incidents are scattered and underdeveloped, especially with regard to the roles and responsibilities, and they do not integrate all possible sources of incident reporting;
    - incidents related to information security are classified under headings that are too general, or are misclassified, and little information is recorded on their nature;
    - users are not made aware of the fact that they must report information security incidents and vulnerabilities; and

  - no incident analysis is performed in a perspective of continuous improvement of security mechanisms.
- In recent years, the City of Québec performed a few information security awareness-building activities, but in general deployed little effort to implement information security as a culture.
- The City did not develop an information security awareness plan based on a rigorous needs analysis and adopted at a high enough hierarchical level to ensure its implementation throughout the organization.
- In the last three years, very few organizational training activities were targeted and followed up on with regard to information security.
- The responsibilities of critical information security stakeholders, such as the Branch, the responsibility holders, the managers and the digital information security officer (*responsable de la sécurité de l'information numérique* – RSIN), are not defined. Out of five policies framing information security:
  - only one mentions the responsibilities of the Branch, and these are not explicitly stated;
  - none give responsibilities to the responsibility holders (only the Directive describes them); and
  - only three mention the responsibilities resting with the managers.
- Management does not adequately monitor information security. First, it has not defined its monitoring needs or management indicators to measure performance in terms of information security. It receives very little management information.

Audit Recommendations

- The Branch should reinforce the governance of information security by:
  - adopting a global information security policy, in order to:
    - specify its expectations in the matter as well as the responsibilities of the stakeholders, and
    - provide for coordination mechanisms to ensure consistent handling of all aspects of security;
  - diligently monitoring the operation and efficiency of all information security components and following up on residual risks.
- The information technologies department (*Service des technologies de l'information* – STI) should support City Management by suggesting guidance in order to implement the necessary foundations for appropriate governance of information security, i.e.:
  - for categorization of information and designation of responsibility holders:
    - attribution of clear responsibilities in this regard and reinforcement of the accountability of designated responsibility holders;
    - adoption of rules to ensure categorization is properly done and used to adequately protect digital information;
  - for risk management:
    - integration of information security in the City's risk management;
  - for the digital information security management system:

- developing an information security implementation plan based on a risk assessment and that states, for each activity, who is responsible, the level of effort planned and the deadline;
- collecting and analyzing the necessary information to support information security management and report on it;

- for awareness-building and training of users and officers:
  - establishing and prioritizing the needs in terms of information security awareness-building and training;
  - developing an employee awareness-building plan stating which activities are planned, which clienteles are targeted and what the timetable is, as well as who is responsible for implementing them and what resources are required to do so.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

An Independent Audit of the Regional Transportation Management Centre's Cybersecurity Controls

Publication Date: 2017

Audit Office: Office of the Auditor General of British Columbia

Link to full report:

http://www.bcauditor.com/pubs/2017/independent-audit-regional-transportation-management-centres-cybersecurity-controls

Audited Organization

- Ministry of Transportation and Infrastructure – Regional Transportation Management Centre (RTMC)

Audit Objective

- To determine whether the Ministry of Transportation and Infrastructure has established appropriate cybersecurity controls to protect its traffic management systems.

Audit Criteria

- The Ministry maintains and manages an inventory of authorized and unauthorized devices and software.
- The Ministry establishes and manages the security configurations for hardware and software on all devices.
- The Ministry continuously validates systems through vulnerability assessments and remediation.
- The Ministry controls and manages the use of administrative privileges.

Main Audit Findings

- Security controls at the RTMC were not strong enough to properly protect its systems from cybersecurity threats. This puts systems at risk of internal and external attacks.
- The Ministry did not update and maintain a complete inventory of authorized and unauthorized devices and software.
- The Ministry did not have a way of detecting and reporting what was running on its network.
- The Ministry had not established baseline configurations standards for all its systems.
- A configuration management system was not in place to continually manage and update the baseline configuration settings of critical systems, and monitor them for configuration changes.

- The Ministry performed a vulnerability scan when the RTMC was first established, but there was no ongoing process for vulnerability assessment and remediation.
- The Ministry lacked proper controls over the system administrative accounts.

Audit Recommendations

- The Ministry of Transportation and Infrastructure should conduct risk assessments of the RTMC operational environment and ensure appropriate security controls are implemented.
- The Ministry of Transportation and Infrastructure should maintain an inventory of all system components (hardware and software) authorized to access the RTMC networks and implement mechanisms to discover any unknown components on the network.
- The Ministry of Transportation and Infrastructure should establish and maintain secure baseline configurations for all RTMC system components.
- The Ministry of Transportation and Infrastructure should conduct ongoing vulnerability assessments and remediation for RTMC systems.
- The Ministry of Transportation and Infrastructure should ensure that the use of system administrative accounts for RTMC systems is properly controlled.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Independent Electricity System Operator—Market Oversight and Cybersecurity

Publication Date: 2017

Audit Office: Office of the Auditor General of Ontario

Link to full report:

http://www.auditor.on.ca/en/content/annualreports/arreports/en17/v1_306en17.pdf

Audited Organization

- Independent Electricity System Operator (IESO)

Audit Objective

- To assess whether the Independent Electricity System Operator had effective systems and processes in place to ensure that:
  - oversight of electricity market participants is sufficient and market participants operate in accordance with market rules; and
  - critical IT assets and infrastructure are protected so that the reliability of the grid is maintained.

Selected Audit Criteria

- Appropriate procedures, controls and processes are in place to detect security attacks, threats, weaknesses and vulnerabilities, and assess their impact on IESO's security posture while supporting key program objectives.

Main Audit Findings

- The IESO does not have a designated senior executive responsible for cybersecurity. The person with the most responsibility for cybersecurity does not have the authority to make the decisions needed to ensure the IESO has sufficient cybersecurity measures in place.
- The number of cybersecurity staff is under the recommended level. At the time of the audit, the IESO had four cybersecurity staff, a number that had not increased over the past decade. Two external consultants who conducted separate reviews of the IESO's IT environment in 2015 and 2016 recommended that IESO should have at least seven dedicated cybersecurity staff.
- The IESO does not have an independent cybersecurity department with clearly defined roles and responsibilities. It is up to IT project managers to decide whether and when to involve cybersecurity

staff in IT planning. In a number of instances, project managers involved cybersecurity staff only in the later stages of projects.

- The IESO cybersecurity systems do not monitor the activities of privileged users in real time to proactively trigger alerts for unusual behavior. Also, the IESO's systems cannot support real-time analysis and investigation of certain types of breaches.
- The cybersecurity team does not review the external vendor contracts and does not assess on an ongoing basis the security risk of external vendors.
- The tapes on which the IESO stores system back-up information are not encrypted. Also, some back-up tapes are stored on-site.

Selected Audit Recommendations

- To strengthen its cybersecurity governance, IESO should create a senior-level position for cybersecurity and establish a formal reporting process to both IESO executives and the IESO Board of Directors.
- To ensure there are sufficient cybersecurity resources in place to respond to cyberattacks, IESO should increase the number of cybersecurity staff to the recommended level of seven and/or engage an external IT cybersecurity vendor to be on standby.
- To reduce cybersecurity risk and to prevent potential costly IT project redesigns, the IESO IT department should involve its cybersecurity staff in the early stages of all IT projects that could pose cybersecurity risks.
- To reduce its cybersecurity risk, IESO procure technology that prevents and identifies breaches of confidential information and monitors staff access to confidential information in real time.
- To reduce its cybersecurity risk, IESO should:
    - establish an external vendor cybersecurity policy; and
    - ensure that its cybersecurity team conduct a regular assessment of the security risk that external vendors pose to the IESO.
- To ensure that backup tapes are adequately protected and available when needed, IESO should:
    - properly encrypt all backup tapes; and
    - store them in a secure off-site location.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

IT Security for Industrial Control Systems in Alberta's Oil and Gas Industry

Publication Date: 2016

Audit Office: Office of the Auditor General of Alberta

Link to full report:

https://www.oag.ab.ca/webfiles/reports/OAGFeb2016Report.pdf

Audited Organizations

- Department of Energy
- Alberta Energy Regulator
- Department of Justice and Solicitor General

Audit Objective

- To determine if the Department of Energy and Alberta Energy Regulator understand the risks from unsecured ICS, and what, if any, role they should play in ensuring those risks are adequately mitigated.

Audit Criteria

- The Department of Energy and Alberta Energy Regulator (AER) understand whether there are threats, risks and impacts to Albertans because of unsecured ICS.

Main Audit Findings

- The Department of Energy and AER have not assessed IT security risks to ICS in Alberta's oil and gas infrastructure. The Department does not believe it is responsible for determining whether ICS risks to provincially regulated oil and gas infrastructure should be assessed. The AER asserted it does not currently have a role in assessing risks with ICS or IT security standards for Alberta's oil and gas industry.
- The Department of Justice and Solicitor General gathers intelligence to identify security threats to Alberta's critical infrastructure. It has assessed the threat of attacks on Alberta's oil and gas industry as low, but it has not assessed what the risks or impact might be if there was a successful attack on Alberta's oil and gas infrastructure.
- The audit team was unable to obtain any documentation from any provincial entity to show that an assessment of the possible risk and impacts from an attack on unsecured ICS was completed.

Audit Recommendation

- The Department of Energy and Alberta Energy Regulator should work together to determine whether a further assessment of threats, risks, and impacts to industrial control systems used in provincially regulated oil and gas infrastructure would benefit Alberta.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Security of Critical Infrastructure Control Systems for Trains

Publication Date: 2016

Audit Office: Victorian Auditor-General's Office

Link to full report:

https://www.audit.vic.gov.au/sites/default/files/20161109-Security-ICS.pdf

Audited Organizations

- Department of Economic Development, Jobs, Transport and Resources
- Public Transport Victoria (PTV)
- Metro Trains Melbourne
- V/Line Proprietary Limited
- Victorian Rail Track
- Emergency Management Victoria

Audit Objective

- To assess whether security risks to critical infrastructure control systems that operate and control train services are managed effectively.

Audit Criteria

- Appropriate levels of governance over control systems have been established.
- Processes and controls to identify, prevent, detect and respond to security events in control systems are effective.
- Business continuity and disaster recovery capabilities are effective and there are established response capabilities.
- Transport agencies have implemented recommendations raised in our 2010 audit Security of Infrastructure Control Systems for Water and Transport.

Main Audit Findings

- PTV has not yet developed a cyber security strategy for control systems.
- Now that the Systems and Information Services Division has been disbanded, it is not clear who is responsible for managing and supporting control systems, and train operators' activities and projects for control systems have not been coordinated.

- There is a lack of understanding about the ownership of control system assets and responsibility for these assets. Instances were noted where PTV, train operators and Victorian Rail Track (VicTrack) could not clearly show which agency owned and had responsibility over control systems. This has led to some activities overlapping and some being omitted, including:
    - PTV and train operators duplicating frameworks, policies and procedures
    - train operators duplicating engineering and maintenance support resources
    - limited management of the security of control systems.
- The audit team reviewed the agreements between PTV and train operators and found that security of control systems is not included as a requirement. As a result, there are no minimum security standards for control systems that train operators need to implement and maintain.
- The lack of clarity about which agency owns and has responsibility for control systems has resulted in maintenance of and upgrades to control systems not being a funding priority.
- Before the audit, PTV had not developed policies or provided guidance to train operators. Instead, effort was being duplicated as train operators had independently started to develop security frameworks, policies and procedures, which were at varying stages of development.
- The board of PTV has limited oversight of vulnerabilities, threats and risks to control systems. The audit found:
    - little evidence of reporting on cyber security issues to the board—PTV had only once provided high-level reporting about cyber security to its board, in April 2016
    - limited board involvement in matters concerning the cyber security of control systems.
- There is no clear responsibility for providing direction or support for the cyber security of control systems at the executive management level within PTV.
- Train operators and PTV should be more active in undertaking audits on the security of control systems. Since its establishment, PTV has only carried out one audit, in January 2016, which evaluated the security framework for control systems of both train operators and itself. Train operators need to implement programs to regularly carry out vulnerability assessments and tests to assess the security of their control systems.
- The security frameworks that train operators have in place do not adequately safeguard the control systems that operate train services. The security controls used to identify, prevent, detect and respond to cyber threats are not able to prevent unauthorized access to the operators' control systems.
- Serious security vulnerabilities in the control systems were identified, which could expose them to cyber threats.

Selected Audit Recommendations

Public Transport Victoria should:

- formalize governance arrangements with train operators and determine responsibilities for the cyber security of control systems.
- prepare a cyber security strategy for control systems that establishes:
    - the desired level of security

    - governance arrangements that ensure adequate oversight.
- establish funding arrangements for control system upgrades, renewals and maintenance as part of the renegotiation of franchise and service agreements.
- identify and appoint a team of suitably qualified and experienced professionals to provide advice to the train operators on security, risk and business continuity management.
- advise train operators on how to implement appropriate risk management systems that identify, measure and monitor control system risks, by:
    - setting up a risk register
    - performing a risk analysis of identified security vulnerabilities to determine whether to immediately introduce security controls and/or technical fixes
- advise train operators on how to implement appropriate compliance management systems that include:
    - processes to monitor, measure, evaluate and report on the performance of security controls
    - internal audit programs to regularly carry out vulnerability assessments or security tests to validate train operators' control system security
- Set up a security controls framework that aims to identify, detect, prevent and respond to cyber threats and that:
    - clearly defines minimum requirements and key performance indicators
    - includes requirements for monitoring and reporting security incidents
    - includes a schedule of audits
    - requires staff training in security of control systems

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Central Services—Web Application Security Requirements

Publication Date: 2016

Audit Office: Provincial Auditor of Saskatchewan

Link to full report:

https://auditor.sk.ca/pub/publications/public_reports/2016/Volume_1/06_Central Services_Web Security.pdf

Audited Organization

- Ministry of Central Services

Audit Objective

- To assess whether the Ministry of Central Services had security requirements that were consistent with best practices for the development and operation of government ministry web applications.

Audit Criteria

- The audit criteria and sub-criteria are listed in Figure 3 of the audit report.

Main Audit Findings

- We found that Central Services did not have complete information on the nature and extent of web applications that it hosts on behalf of the ministries. At December 2015, its list of web applications did not include all ministry web applications that Central Services hosted and that are subject to its Security Policy, nor all key details about the web applications (e.g., risk classification, software version, server the applications runs on).
- At December 2015, Central Services' Security Policy had limited supporting procedures and guidance to help staff from the ministries, including its own staff, interpret and implement sections of its overall Security Policy that relate to web applications.
- Overall, although Central Services set out security requirements in its Security Policy, it did not set out supporting procedures and guidelines in many key areas related to IT security for web applications.
- Central Services intends to revisit its Security Policy at least every two years. It had not set out how often it planned to update its procedures and guidelines.
- Central Services did not have procedures to ensure web developers had access to written updates about evolving security weaknesses identified by industry, so they could consider these when developing new web applications.

- Central Services does not complete routine testing of web application vulnerabilities, or require the ministries to do so. Rather Central Services may carry out or contract for these tests only upon request of the ministries. Instead of a proactive approach to routinely testing the adequacy of the security of the Ministries' web application vulnerabilities, Central Services used a reactive approach.
- In the test of 18 websites, over 1,400 vulnerabilities were identified. One website had over 100 high-risk vulnerabilities; overall, 22% of the vulnerabilities identified were classified as medium and/or high risk. A well-known high-risk weakness was identified in 10 of the 18 ministry websites that were tested. Weaknesses were widespread across the ministries; they were identified in 17 of the 18 ministry websites that were tested. Most of the tested websites were not sufficiently secure.

Audit Recommendations

- The Ministry of Central Services should document key information about all ministry web applications that are subject to its security policy.
- The Ministry of Central Services should develop and maintain comprehensive procedures and guidelines to support the development and operation of secure web applications.
- The Ministry of Central Services should require routine analysis of web application vulnerabilities to monitor compliance with its security policy.
- The Ministry of Central Services should work with the ministries to address identified higher-risk web application vulnerabilities.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Central Services—Data Centre Security

Publication Date: 2016

Audit Office: Provincial Auditor of Saskatchewan

Link to full report:

https://auditor.sk.ca/pub/publications/public_reports/2016/Volume_1/05_Central Services Data Centre Security.pdf

Audited Organization

- Ministry of Central Services

Audit Objective

- To assess whether the Ministry of Central Services had effective processes to secure the data centre. (The audit did not assess the effectiveness of security control for specific client applications).

Audit Criteria

- The audit criteria and sub-criteria are listed in Figure 3 of the audit report.

Main Audit Findings

- Central Services continues to lack information from clients about the classification (e.g., level of sensitivity) of the data residing on servers within the data centre. Central Services needs this information so that it can work with its clients to determine the appropriate security level for the data (i.e., provide stronger security controls for confidential information such as social insurance numbers).
- By December 2015, Central Services had not finished documenting which client data resides on which particular servers. It also had not established separate parts of the network to differentiate security controls based on data classification.
- Central Services used firewalls to help protect its data centre from hackers. Central Services located data centre firewalls at appropriate locations, and monitored reported security events. However, the firewalls (at the data centre and at client locations) were not properly configured. For example, Central Services' data centre firewall rules did not sufficiently restrict access to the data centre because Central Services did not effectively define the firewall rules that its service provider must follow.

- In addition, firewalls at client locations and network devices (e.g., switches) were not receiving software updates, or were no longer receiving user support. This means these devices were not patched for known vulnerabilities, dating back to 2013 for client firewalls.
- At December 2015, Central Services noted over 100 of the 1,000 servers, which it manages on behalf of clients, used unsupported versions of operating software. Central Services worked with some clients during 2015 to upgrade servers and databases to vendor supported levels. However, by December 2015, not all clients had formally documented their acceptance of the risk related to unsupported components.
- Although Central Services' data centre service provider updated most servers, on at least a quarterly basis, the audit team found patching on all servers was not complete for all known vulnerabilities. All 10 servers tested by the audit team were missing updates (some related to updates made available in 2012). Central Services did not ask its staff or its service provider to do these updates. Also, it did not have a documented risk analysis as to why these servers did not need the missing updates.
- As in prior years, Central Services did not have a complete and tested disaster recovery plan for the data centre. As a result, some of Central Services clients with critical client systems do not have disaster recovery plans. A few Central Services' clients have signed separate disaster recovery agreements with other service providers to restore specific critical systems and data if a disaster occurs. However, having multiple agreements for disaster recovery does not result in an effective enterprise approach to disaster recovery for the data centre.
- By December 2015, Central Services used more secure methods for accessing systems and data. Network accounts complied with its password standards.

Audit Recommendations

- This audit reviewed progress made in implementing previous (2012) audit recommendations. Two recommendations were not fully implemented and remained valid after the follow-up audit:
    - The Ministry of Central Services should adequately configure and update its server and network equipment to protect them from security threats.
    - The Ministry of Central Services should have a disaster recovery plan for the data centre and client systems.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Malware in the WA State Government

Publication Date: 2016

Audit Office: Office of the Auditor General of Western Australia

Link to full report:

https://audit.wa.gov.au/wp-content/uploads/2016/12/report2016_28-Malware.pdf

Audited Organizations

- Department of Agriculture and Food
- Department of the Attorney General
- Main Roads Western Australia
- Department of Mines and Petroleum
- Department of the Premier and Cabinet
- Department of Transport

Audit Objective

- To determine whether selected government agencies have effective controls to prevent, detect, and respond to malware threats and malicious software infecting their computer systems.

Audit Criteria

- Agencies have implemented controls to prevent, detect and respond to malware threats
- Controls are effective at managing malware threats

Main Audit Findings

- The audit found malware related communication on all the networks that were tested. This included attempted attacks by malicious web pages, downloads of malware files and active malware communicating out to the internet. The high volume of attacks shows a committed threat that is working to defeat security controls and a need for agencies to understand the threats and fix any gaps in their security controls.
- Two agencies had signs of persistent malware infections that had bypassed their security controls. One agency had a single infection that was active for most of the 12-day sample period. Another agency had more than 5 infections active for approximately 2 days, with at least 1 computer reinfected during the assessment period. These active infections placed the agency networks, systems and data at risk.

- IT control failures are still common. Testing revealed all agencies had some control failures, or missing controls. Common issues were around missing security patches and outdated operating systems. Problems were also noted with management of antivirus software, assignment of access rights, and network design.
- Skilled professionals are required to monitor the IT environment and identify issues proactively. All of the selected agencies had IT staff working in information security roles. Some were fortunate to have more than one, however most represent a single point of reliance, and failure.
- Most agencies did not provide adequate awareness training for their staff.
- The WA Government lacks a coordinated approach to cyber threats, including malware.
- At the time of the audit, there was no whole-of-government security policy or framework providing guidance to agencies on how to implement a successful security program.
- Agencies are also not required to report malware incidents to a central agency. No single body could provide the audit team with an overview of the size or nature of the malware threat faced by agencies.

Audit Recommendations

- Audited agencies should:
    - Assess the risk posed by the malware threats observed during the audit.
    - Improve any controls that were identified as ineffective.
    - Consider additional controls to better secure their networks, systems and data against malware.
- The public sector, by way of the Office of the Government Chief Information Officer, should:
    - Consider methods to foster collaboration, information and resources sharing between agencies.
    - Gather information to properly understand the threat posed by malware and other cyber threats to the public sector.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Security Management of Information Systems

Publication Date: 2016

Audit Office: Auditor-General's Department, South Australia

Link to full report:

https://www.audit.sa.gov.au/LinkClick.aspx?fileticket=VVFWud381CQ%3d&tabid=369&portalid=0&mid=970&forcedownload=true

Audited Organizations

- Department for Education and Child Development
- Urban Renewal Authority (Renewal SA)
- South Australian Fire and Emergency Services Commission (SAFECOM)
- Court Administration Authority (CAA)
- Department of Planning, Transport and Infrastructure (DPTI)
- Public Trustee
- Department for Environment, Water and Natural Resources (DEWNR)
- South Australian Water Corporation (SA Water)
- Attorney-General's Department (AGD)
- Department of the Premier and Cabinet (DPC)

Audit Objective

- To determine whether agencies were effectively managing the following aspects of information security:
    - Legacy server operating systems
    - Patch management (operating systems and selected databases)
    - Privileged user access management
    - Mobile devices
    - Application whitelisting.

Audit Criteria

- Not publicly available

Main Audit Findings

- Eight of the 10 reviewed agencies were operating unsupported legacy servers. There were 233 legacy servers in operation across the 10 agencies (13% of all servers operating at these agencies).
- All agencies are working to decommission their legacy servers. However, the risk exposure and extent of mitigating controls applied to protect these servers varies between agencies. Several agencies have not implemented sufficient mitigating controls in the interim.
- Most reviewed agencies had defined policies and procedures to manage the patching process. However, there were servers with missing operating system or database security update patches at three of the four agencies reviewed. Additionally:
    - a core information system application, database and operating system was not patched at one agency
    - two agencies had deficiencies in their patch management and change management policies/procedures
    - there were deficiencies in patching compliance checking processes and reporting
    - there was insufficient documentation of patching exemptions at one agency.
- The two reviewed agencies were not effectively managing privileged user access to Active Directory in line with the Information Security Management Framework requirements. There were instances of potentially excessive domain-level privileged access and privileged access permissions on local computers. There was also:
    - no formal periodic review of Active Directory privileged users
    - deficiencies in user access and IT security policy/procedure(s)
    - cases of terminated employee reports that were not received or reviewed promptly
    - privileged user activities that were not sufficiently logged and monitored.
- The two reviewed agencies should improve controls to effectively manage the use of mobile devices to access agency resources and data. Although both agencies had defined policies and procedures to manage mobile devices, the audit found that:
    - security controls applied to mobile devices did not meet best practice guidelines
    - mobile access was not restricted by individual device
    - there was insufficient reporting of agency mobility usage
    - mobile devices policies and procedures were not regularly reviewed or approved.
- The two reviewed agencies had not implemented application whitelisting. The audit also found that:
    - periodic application reviews are not performed at one agency and documentation of them is not retained at another agency
    - information security policies at one agency are in draft, pending review and approval.

Selected Audit Recommendations

- Agencies should decommission legacy Windows servers as soon as practicable.
- Until decommissioned, agencies should consider implementing additional controls to mitigate the increased risk of continuing to operate legacy servers. This should include:

  - implementing application whitelisting on the server
  - avoiding the use of privileged accounts on servers for non-administrative activities
  - implementing a third-party software-based application firewall, or a 'virtual patching' solution using an intrusion detection/prevention system
  - disabling unneeded functionality (such as non-essential services) or common intrusion methods.
- Agencies should:
  - review servers identified with missing patches and ensure that they apply all applicable security patches
  - ensure that they identify patching requirements promptly, through regular review of security bulletins
  - document policies for patch management and change management. Ensure that policies and procedures are reviewed regularly and updated as required
  - ensure that assurance practices include regularly assessing patching compliance levels for servers and workstations
  - retain sufficient documentation of patching exemptions for all servers.
- Restrict access to local administrator rights based on user duties.
- Ensure that separate accounts are established to segregate standard and administrative user activities.
- Document a policy for user access management. Ensure that IT policies and procedures are reviewed regularly and updated as required.
- Ensure that terminated employee reports are provided regularly and promptly. Once provided, agencies should review the reports and delete applicable user accounts as soon as practicable.
- DPC should provide additional guidance to agencies about implementing mobile device management (MDM) software or other technical controls.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

SaskPower—Managing the Risk of Cyber Incidents

Publication Date: 2015

Audit Office: Provincial Auditor of Saskatchewan

Link to full report:

https://auditor.sk.ca/pub/publications/public_reports/2015/Volume_1/18_SaskPower-Cyber Incidents.pdf

Audited Organization

- SaskPower

Audit Objective

- To assess whether SaskPower had effective processes to manage the risk of cyber incidents for the protection of the provision of power.

Audit Criteria

- The audit criteria and sub-criteria are listed in Figure 1 of the audit report.

Main Audit Findings

- While SaskPower kept a current listing of what it had assessed as its critical assets, it had not specifically identified which of those assets could be potential targets for a cyber incident.
- In March 2015, SaskPower provided its senior management and Board of Directors with a high-level summary of the potential threats it faced in relation to its assets that provide power, the impact of those threats, and the safeguards that it had in place to mitigate those threats (mitigation strategy). However, this high-level summary may not be complete. SaskPower did not specifically identify potential weaknesses in and threats to its Operational Technology systems (e.g., unauthorized connections of these systems to the internet, use of USBs) that may allow an attacker to get into the critical cyber assets. In turn, SaskPower did not assess the likelihood of these types of cyberattacks that potentially could lead to a cyber incident.
- SaskPower has a detection and response plan for use in the event of an incident, including a cyber incident. This plan includes detailed procedures for both detecting and responding to cyber incidents. The plan sets out expected detection activities, such as use of intrusion detection systems and anti-virus software and the review of security logs and alerts. SaskPower has implemented the detection

activities as set out in the plan, including periodic reviews of system logs and alerts. Various staff were assigned responsibility to review security logs and alerts.

- While SaskPower used processes to detect and track various IT security-related events, the audit team found that it did not have documented criteria that set out what IT security-related events it considered as cyber incidents (such as a series of failed log-in attempts in a short period).
- SaskPower followed its user–access change procedures and appropriately restricted its administrative user access for its critical assets to a small number of employees.
- SaskPower communicated its response plan procedures to its employees and has made it readily available to staff for reference should an incident occur.
- The incident response plan requires yearly training of the response team and a review of the incident response to incorporate lessons learned in future responses. There was evidence that yearly training occurred. SaskPower regularly tests its response plan through test exercises.

Audit Recommendations

- SaskPower should document the most likely types of information technology threats that could lead to cyber incidents that would adversely impact its ability to provide power.
- SaskPower should confirm that its cyber risk mitigation strategy addresses the significant threats of cyber incidents that would adversely impact its ability to provide power.
- SaskPower should provide its staff with guidance to assist in assessing when an information technology security-related event is considered a cyber incident and requires the use of its incident command system response plan.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Manitoba Hydro—Managing Cyber Security Risk Related to Industrial Control Systems

Publication Date: 2014

Audit Office: Office of the Auditor General of Manitoba

Link to full report:

http://www.oag.mb.ca/wp-content/uploads/2014/03/Chapter-8-Manitoba-Hydro-ICS-Security-Web.pdf

Audited Organization

- Manitoba Hydro

Audit Objective

- To determine whether Manitoba Hydro's risk management practices ensure the design of security controls over industrial control systems and related information technology reasonably mitigate identified cyber risks.

Audit Criteria

- Audit criteria were based on the standards included in the *IT Risk Management Audit/Assurance Program* developed by the Information Systems Audit and Control Association (ISACA).

Main Audit Findings

- Manitoba Hydro has not prioritized its Industrial Control Systems (ICS) and related IT systems for criticality to its generating, transmitting and distributing processes. The ICS cyber security risk has not been identified as a corporate risk profile and has not been assessed. As such, it has not been communicated to the Board. Risk reports were not produced by divisions within Power Supply and IT Services.
- Manitoba Hydro has not identified and prioritized all ICS and related IT systems that are used to support its generating, transmitting and distributing processes. Nor has it created a related inventory of all ICS hardware and software.
- At each of the six sites visited by the audit team, some ICS security controls were evident (for example perimeter physical security, password controls, and computer room environmental controls) but serious weaknesses were identified in the following areas:
    - Network segmentation.
    - Patch management.

  - Access controls.
  - System hardening.
  - Intrusion detection.
  - Physical security.
  - Malware protection and detection.
  - Change controls and configuration management.
  - Incident planning and response.
- While an "air-gap" reduces the risk of malware spreading from a generation station to the SCC and vice versa, it has fostered a false sense of security within Manitoba Hydro. This configuration is used at all of the facilities visited during the audit. In today's cyber threat environment, an "air-gap" between two networks should not be seen as an all-encompassing security control. Additional layers of controls are essential to reducing overall risks.
- At Manitoba Hydro, there is no corporate-wide oversight on the quality and adequacy of cyber security measures in place. Each business unit and department is responsible for managing their ICS systems and risks, potentially understating corporate-wide risks. Fragmented control can result in inconsistent practices/controls.
- Because of potential operational and safety concerns, the corporate IT policies do not apply to ICS systems. No other policies are in place to guide operating divisions in managing and securing their ICS systems.
- During site visits it was noted that each site had some physical security controls restricting public access but controls were inconsistently applied increasing the risk of unauthorized access to ICS systems. The rationale for the varying physical security measures at each site could not be provided.
- The cyber security awareness training provided by Manitoba Hydro does not sufficiently cover ICS threats and vulnerabilities. In addition, corporate security awareness communications do not deal with ICS cyber security risks.

Audit Recommendations

Manitoba Hydro should:

- identify, assess and mitigate all ICS cyber security risks – this should be performed on a priority basis for assets critical to operations.
- once ICS cyber security risks have been assessed, include cyber security as a corporate risk profile in the annual risk management report that is presented to the board.
- assign responsibility for corporate-wide cyber security to one executive.
- develop and implement ICS cyber security policy instruments and make them applicable to all ICS systems.
- assign responsibility for corporate-wide physical security to one executive.
- develop and implement physical security policy instruments to control physical access to ICS systems.
- develop and deliver a comprehensive ICS cyber security training and awareness program for all staff responsible for the operation, maintenance and security of ICS systems.
- develop a strategy to converge IT and Operations Technology management, including IT security.

Focus On Series – IT Security

Audit Summary

Audit Title
Security of Wireless Networks

Publication Date: 2014

Audit Office: Office of the Auditor General of the City of Montréal

Link to full report:

http://www.bvgmtl.ca/wp-content/uploads/2014/06/2013AR_section5-4.pdf

Audited Organizations

- Service des technologies de l'information (STI)
- Division des ressources informationnelles, Saint-Laurent borough
- Division de l'informatique, St-Léonard borough

Audit Objective

- To determine if the controls that were put in place ensure that only duly authorized wireless networks are present within the city and that their security mechanisms prevent unlawful access to the city's corporate network.

Audit Criteria

- Detailed criteria are not publicly available, but the sources of the criteria are provided:
    - *Recommandations de sécurité relatives aux réseaux WiFi*, Agence nationale de la sécurité des systèmes d'information, General Secretariat of Defence and National Security, French Ministry of Defence;
    - *Establishing Wireless Robust Security Networks: A Guide to IEEE802.11i*, Special Publication 800-97, National Institute of Standards and Technology (NIST).

Main Audit Findings

- Overall, the wireless networks were adequately protected. However, management of wireless security needs some improvement.
- The STI has no process in place to detect unauthorized wireless networks. The audit team found a wireless access point concealed in a city building and were unable to establish who owned it.
- The audit team uncovered several open and unsecured wireless access points in two of the eight buildings that were sampled.

- The audit team uncovered nine wireless access points that were configured to use the WPA2 security protocol but that also allowed the use of less robust protocols, including WPA and WPS (in five buildings).
- The audit team uncovered two printers in one building whose wireless functionality was activated but not protected. These printers were being used by employees who handle confidential information.

Audit Recommendations

- The Service des technologies de l'information should:
    - implement a recursive process to detect unauthorized wireless networks and, where necessary, to take the corrective action needed to remove them.
    - ensure that all wireless access points are configured with a robust security protocol.
    - ensure, with the relevant boroughs, that wireless network equipment use only the most robust security protocols.
    - deactivate its printers' wireless access functionality if it is not absolutely required. In cases where such access is required, it should activate a robust security protocol.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Cyber Attacks: Securing Agencies' ICT Systems

Publication Date: 2014

Audit Office: Australian National Audit Office

Link to full report:

https://www.anao.gov.au/sites/g/files/net4181/f/AuditReport_2013-2014_50.pdf

Audited Organizations

- Australian Bureau of Statistics (ABS)
- Australian Customs and Border Protection Service (Customs)
- Australian Financial Security Authority (AFSA)
- Australian Taxation Office (ATO)
- Department of Foreign Affairs and Trade (DFAT)
- Department of Human Services (DHS)
- IP Australia

Audit Objective

- To assess selected agencies' compliance with the four mandatory ICT security strategies and related controls in the Australian Government Information Security Manual (ISM).

Audit Criteria

- The mandatory ISM controls that support the top four mitigation strategies have been implemented.
- Effective logical access and change management processes to authorize the implementation of critical security patching for application and operating systems are being used.
- Approved dispensations are in place for any non-compliance with the mandatory ISM controls.

Main Audit Findings

- The audited agencies had established internal information security frameworks, implemented controls designed to safeguard the enterprise ICT environment from external cyber attack, and had stipulated change management processes to authorise the implementation of security patches for applications and operating systems. While these arrangements contributed to the protection of agency information, the selected agencies had not yet achieved full compliance with the top four mitigation strategies mandated by the Australian Government in 2013; Further, none of the selected agencies were expected to achieve full compliance by the Government's target date of mid–2014.

- Based on their stage of implementation of the top four mitigation strategies and IT general controls, the selected agencies' overall ICT security posture was assessed as providing a reasonable level of protection from breaches and disclosures of information from internal sources, with vulnerabilities remaining against attacks from external sources to agency ICT systems.
- Three of the seven agencies had implemented application whitelisting across the desktops, while one agency was also actively implementing application whitelisting across its servers. The ANAO raised concerns when it observed, in the case of two agencies, that their application whitelisting was set to 'audit only mode', which simply logged events that application whitelisting would have blocked, had it been enabled. In the case of four agencies, the default policy was not set to deny the execution of software, potentially enabling staff without administration rights to load software on agency systems.
- In all cases, agencies were non- compliant with the requirements to apply critical security patches within two days from the release of the patches, and only two agencies had demonstrable patching practices enabling them to respond to vendors' routine or ad hoc patch releases, such as Microsoft's monthly security patch release.
- The ANAO's assessment of agency policies to capture and maintain audit logs for privileged user accounts found that in most cases the policy was not enforced. This is a systemic control weakness that raises questions as to how effectively agencies can identify, respond to, or investigate unauthorised access to privileged user accounts, or inappropriate activities by privileged users.

Audit Recommendations

- To achieve full compliance with the mandatory ISM strategies and related controls, agencies should:
  - complete activities in train to implement the top four ISM controls across their ICT environments; and
  - define pathways to further strengthen application whitelisting, security patching for applications and operating systems, and the management of privileged accounts.
- To reduce the risk of cyber attacks to information stored on agency databases, agencies should strengthen logical access controls for privileged user accounts to the database by eliminating shared accounts, recording audit logs and monitoring account activities.
- To strengthen their ICT security posture, agencies should:
  - conduct annual threat assessments across the ICT systems, having regard to the Top 35 Mitigations Strategies—as proposed by the Australian Signals Directorate; and
  - implement periodic assessment and review by the agency security executive of the overall ICT security posture.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

WoVG Information Security Management Framework

(note: "WoVG" means Whole of Victorian Government)

Publication Date: 2013

Audit Office: Victorian Auditor-General's Office

Link to full report:

https://www.audit.vic.gov.au/report/wovg-information-security-management-framework

Audited Organizations

- Department of the Premier and Cabinet
- Department of State Development, Business and Innovation (DSDBI)
- Department of Treasury and Finance
- Department of Human Services
- Department of Justice
- CenITex
- State Revenue Agency
- Treasury Corporation of Victoria
- Victorian Funds Management Corporation
- IT Shared Solutions

Audit Objective

- To assess the effectiveness of ICT security policy, standards and protection mechanisms for the state's ICT systems and data.

Audit Criteria

- Appropriate information security policy direction and guidance is in place to provide consistent protection to state ICT systems and data.
- Central agencies have oversight of, and coordinate responses to, WoVG information and system threats.
- Selected agencies have established and complied with information security policy, standards and processes.

Main Audit Findings

- An appropriate information security policy and framework is in place, but it only applies to 20 inner WoVG agencies. Other public sector entities, including the outer WoVG agencies in this audit, are not required to conform to any specific policy or standard.
- Apart from certain reporting requirements for inner WoVG agencies and a program of training and briefings, there was no evidence that central agencies took any initiative to help these agencies apply the policy and framework.
- There is no coordination and communication by DSDBI on information security matters with outer WoVG agencies. These agencies do not receive support from central agencies on information security matters. There was also no expectation that agencies develop internal policy and standards, nor was there any guidance on how these agencies should address their information security requirements.
- From a government and central agency viewpoint there is:
    - no visibility of areas where assistance could be provided to minimise the cyber threat risk
    - no ability to assess the risk posed to outer WoVG agency ICT systems in a hostile cyber threat environment
    - no easy way to develop a whole-of-government current threat assessment and risk profile
    - no assurance that outer WoVG agencies are addressing information security matters.
- Inner WoVG agency information security policies were reviewed in 2010, but there was little evidence of any oversight of agency standards, controls and compliance since then.
- Because agencies' reports on cyber attacks they have experienced are not consolidated, there is no central repository for government to analyse the type or incidence of cyber threats or the ability of systems to resist cyber attacks.
- There is neither a central, consolidated view of cyber threats, nor arrangements in place to brief government in the event of a multi-agency or sustained attack.
- Cyber alerts depend on accurate IP information. DSDBI and individual agencies are not managing IP information to ensure correct and current information is available. This is essential for an effective response to detected cyber threats.
- None of the agencies included in this audit has fully complied with government information security policy and standards. However, each of the audited agencies did have some information security policy in place.
- Overall awareness of how public sector ICT systems would perform if subjected to a cyber attack is unsatisfactory. Closer central agency involvement is necessary until an acceptable level of information security maturity is reached across public sector agencies.

Audit Recommendations

- The Department of State Development, Business and Innovation should:
    - send the information security management policy to government for formal consideration
    - amend information security policy and standards to include those outer WoVG agencies operating information and communications technology systems that have an aggregate high

transaction value critical to state revenue, systems critical to public safety, or systems holding sensitive personal data with potential value to third parties
    - require WoVG agencies to report any variations between the information security standards and their agency information security management frameworks, that have been approved by their agency head, as part of the annual information security management framework self-assessment reporting process
    - develop processes for outer WoVG agencies to be included in relevant briefings and information security forums, and to be provided with advice and assistance outside of the WoVG Chief Information Officers Council
- The Department of Premier and Cabinet, and the Department of State Development, Business and Innovation should:
    - confirm their respective roles and responsibilities for information security once the Emergency Management Bill 2013 is enacted
    - confirm that briefings on cyber threats will be made to the State Crisis and Resilience Council by the Department of State Development, Business and Innovation as the agency with primary responsibility for WoVG information and communications technology, and that the State Crisis and Resilience Council will in turn recommend briefings for ministers as appropriate.
- The Department of State Development, Business and Innovation should:
    - arrange for a cyber alert subscription service to be available to every government agency from a suitable provider
    - develop and implement a process for maintaining a register of all IP addresses in use by public sector departments and agencies.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Information Technology (IT) Security Management Practices

Publication Date: 2013

Audit Office: Office of the Auditor General of Manitoba

Link to full report:

http://www.oag.mb.ca/wp-content/uploads/2013/01/WEB-Chapter-3-IT-Security-Mgmt-Practices.pdf

Audited Organization

- Business Transformation & Technology (BTT)

Audit Objective

- To determine whether Business Transformation & Technology designed and implemented adequate Information Technology (IT) security management practices and controls.

Audit Criteria

- Business Transformation & Technology:
  - has processes to identify, assess, mitigate, and accept IT security risks.
  - has information security strategies that support IT and organizational objectives.
  - has policies that address significant IT security risks.
  - updates and communicates IT security policies.
  - classifies and safeguards information assets.
  - ensures that adequate security controls are in place in outsourced services.
  - secures system and network operations to protect against threats and vulnerabilities.

Main Audit Findings

- BTT is not aware of all significant IT security risks; it only recently began to assess some common IT security risks. Much more work is needed to identify and assess risks, decide how to mitigate them, assign accountability, and mobilize resources. The audit team is particularly concerned that risk assessments have not been conducted, nor are any planned, around the operations of the Legislative Building Information Systems (LBIS) unit. BTT practices in the area of IT security risk management have not significantly improved despite previous comments and recommendations.
- BTT has not yet developed an IT strategic plan, including an IT security strategic plan, despite previous comments and recommendations.

- BTT has not implemented an IT Security Policy despite previous comments and recommendations. IT security policy instruments are not in place for the following activities that have associated IT security risks: virtualization, mobile devices, wireless networking, and physical security.
- It has been several years since BTT has engaged the services of an independent third party to conduct an audit of its IT security management practices. The latest review occurred in 2005/06. A report was received in March 2006. The report presented multiple deficiencies and recommendations. BTT did not review the recommendations for appropriateness, develop action plans, and track the implementation of the recommendations.
- The audit team is concerned that the Security Checks policy does not include periodic security checks for current employees. As noted above, checks are required for certain positions only upon commencement of employment. There is no requirement to obtain periodic security checks during employment. This is particularly important for jobs with access to sensitive information assets.
- BTT has not defined minimum password requirements.
- BTT has not defined minimum requirements for creating, maintaining and deactivating access.
- BTT has also not developed requirements for the monitoring of user activities.
- BTT has outsourced the management of its five main data centres but has not defined its physical security requirements. As a result, there are distinct differences in the physical controls implemented at the outsourced data centres. The rationale, including risk assessments, for the physical security controls at each outsourced data centre is not documented.
- The audit team looked at one Contractor's patch levels and found that it was significantly behind on patching high risk security vulnerabilities, leaving systems and data unnecessarily exposed for a prolonged period of time.
- Emails are not encrypted by the sender, increasing the risk of sensitive data being exposed to unauthorized individuals. This is a particular concern because the network is also not encrypted.
- To protect the information on laptop hard drives, BTT uses an encryption method that, according to the vendor, is reasonable for low risk data, but would not be sufficient for highly sensitive data. The Information Protection Centre (IPC) reported that 14 laptops were lost or stolen in calendar year 2011, yet IPC did not determine the sensitivity of the data residing on those laptops.

Selected Audit Recommendations

- BTT should complete, on a priority basis, a comprehensive IT risk assessment, which would include an assessment of IT security risks.
- BTT should complete an assessment of the risks related to the operations of the LBIS.
- BTT should develop an IT strategic plan and a properly aligned IT security plan.
- BTT and IPC should identify performance measures for the management of IT security operations, and set a specific target be for each measure. Once an IT security plan is in place, performance measures and targets should align with the noted security goals and objectives.
- BTT and IPC should provide senior management with quarterly reports that focus on:
    - key performance measures (as agreed to by senior management).
    - performance in relation to the defined targets.

    - actions to address any performance shortfalls in meeting objectives.
- BTT should obtain, at regular intervals, independent third party audits of its IT security practices, and progress reports on the implementation of recommendations should be provided to senior management.
- BTT should strengthen its Policy Management Framework by requiring that IT risk assessments and strategic objectives support the need for new or updated policy instruments.
- BTT should implement an over-arching IT Security Policy.
- Upon the completion of IT security risk assessments, BTT should implement additional IT policy instruments needed to mitigate IT security risks.
- BTT should strengthen its Policy Management Framework by defining the frequency of IT policy instrument review.
- BTT should develop a prioritized schedule or plan for the review and update of all existing IT policy instruments and progress against the plan should be actively monitored.
- IPC should enhance the security awareness program by:
    - incorporating the use of IT security incident trends and documented risks.
    - developing additional security awareness training specifically targeting users in higher risk positions.
    - using additional awareness techniques.
- BTT should obtain periodic assurance that contractors are obtaining security checks on employees with access to government information assets.
- BTT should develop logical access control requirements.
- BTT should develop and implement minimum physical security requirements for data centres.
- IPC should establish standard IT security requirements. Once these are in place, IPC should assess whether the security practices of contractors meet the standard requirements and, if there are gaps, ensure security practices are strengthened.
- IPC should develop and implement a vulnerability assessment methodology.
- Upon completion of IT security risk assessments and the implementation of data classification standards, BTT should implement a data loss prevention strategy.
- IPC should implement email and laptop hard drive encryption methods that appropriately protect all levels of data sensitivity.
- IPC should document, track, and analyze all information security events and incidents.
- IPC should routinely test information security incident management processes and make improvements as required.

Back to Table of Contents

Focus On Series – IT Security

Audit Summary

Audit Title

Securing the JUSTIN System: Access and Security Audit at the Ministry of Justice

Publication Date: 2013

Audit Office: Office of the Auditor General of British Columbia

Link to full report:

http://www.bcauditor.com/pubs/2013/report9/securing-justin-system-access-and-security-audit-ministry

Audited Organization

- Ministry of Justice

Audit Objective

- To assess whether the JUSTIN system is effectively managed to protect against unauthorized access to information in the system.

Audit Criteria

- The system is adequately secured from internal and external threats.
- JUSTIN information breaches are likely to be discovered.

Main Audit Findings

- Attackers could gain access to Ministry of Justice systems, exposing critical JUSTIN information. The Ministry of Justice does not have adequate control over its infrastructure to prevent attackers from reaching and extracting sensitive JUSTIN information.
- There is excessive access increasing the risk of inappropriate disclosure and thereby threatening individuals' privacy and personal safety. The Ministry has provided thousands of JUSTIN users with a level of access extending well beyond "need to know". There are currently 3,300 JUSTIN users with access to entire RCCs, including details of police investigations, witness 'will say' statements, and victim and witness contact information.
- Highly sensitive information is not locked down, compromising its security and confidentiality. Controls have been built into JUSTIN to protect certain information; however, these controls are not used correctly or have been by-passed, allowing open access to sensitive information.
- There is a lack of visibility and ineffective control over copies of JUSTIN information leaving the ministry. Controls are inadequate to detect and or prevent users from making unauthorized copies of

JUSTIN information, and therefore, no way of telling what information may have left the ministry and where it may have gone.

- Failure to detect unauthorized disclosures of JUSTIN information is preventing a proactive response to security breaches. Ministry controls are inadequate to detect unauthorized accesses from internal or external sources. Without proper awareness, proactive response to mitigate damages caused by wrongful disclosures of information is not possible.
- There are JUSTIN users with RCC access who have not had a criminal record check. Only new hires are required by policy to have one. Some IT support staff in organizations supporting JUSTIN have not had criminal record checks.

Audit Recommendations

- Controls in network and system components in the JUSTIN environment should be reviewed, reconfigured, documented and better managed to ensure multiple layers of security are in place.
- User access to JUSTIN information should be granted and managed based on the principle of 'need to know'.
- Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring in place.
- More effective audit trails and tools should be in place to enable detection and investigation of suspicious or unauthorized activity.
- An effective monitoring program should be in place to enable proactive detection of unauthorized access and removal of copied JUSTIN information.

Back to Table of Contents

Appendix 2
Glossary of Selected Information Technology Terms

Access control list (ACL)
With respect to a computer file system, a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as which operations are allowed on given objects.

Application
A computer program, such as word processors, spreadsheets, database programs, and accounting programs.

Application whitelisting
A security control designed to protect against unauthorized and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software can be executed. (The list of programs and software that are granted access to a computer, network, or protocol is called a whitelist.) All programs and software libraries not on the whitelist are prevented from executing.

Business continuity plan
A plan to continue operations if a place of business (for example, an office, worksite, or data centre) is affected by adverse physical conditions, such as a storm, fire, or crime. Such a plan typically explains how the business would recover its operations or move operations to another location. For example, if a fire destroys an office building or data centre, the people and business or data centre operations would relocate to a recovery site.

Configuration
The arrangement or set-up of the hardware and software that make up a computer system.

Cyber attack
A deliberate act through the Internet to manipulate, deny, degrade, or destroy computers or networks, or the information stored in them. The objective of a cyber attack is to seriously compromise security, stability, or prosperity.

Cyber resilience
The ability to continue to provide services while deterring or responding to cyber attacks.

Cyber security risk
The potential for adverse events affecting organizational operations and resources due to unauthorized access, use, disclosure, disruption, modification, or destruction of information, information technology, and/or operations technology.

Cyber threat
The threat of unauthorized access to a control system device and/or network. This access could be directed from within an organization (for example, by a disgruntled employee) or from a remote location by an unknown person (for example, a hostile government, a terrorist group, or a malicious intruder) using the Internet.

Database
A comprehensive collection of related data organized for convenient access in a computer.

Data centre
A central location for computer network hardware and software, especially storage devices for data.

Defence-in-depth
The practice of using layered security mechanisms to increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.

Disaster recovery plan
A documented process or set of procedures to recover and protect a business IT infrastructure in the event of an emergency or a disaster. A disaster recovery plan is part of a larger, organization-wide business continuity plan.

Electronic media
Various types of data storage, including hard drives, compact discs, DVDs, flash memory cards, and USB drives.

Firewall
Software and/or hardware intended to restrict or block access to a network or computer. Firewalls can be set up using firewall rules to allow only certain types of data through.

Hardware
The machines, wiring, and other physical components of a computer or other electronic system.

Hostile actor
An individual or organization, including an agency of a nation state, that conducts cyber attacks.

Information security management system (ISMS)
A management process with a set of policies concerned with information security management or IT-related security and availability risks. The governing principle behind an ISMS is that an organization should implement, design, and maintain a coherent set of policies, processes, and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

Intrusion detection system
A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

Local area network (LAN)
A computer network that interconnects computers within a limited area, such as a home, school, computer laboratory, or office building, using network media. The defining characteristics of LANs, in contrast to wide area networks (WANs), include their smaller geographical area and non-inclusion of leased telecommunication lines.

Logical security
Software safeguards for an organization's systems, including user identification and password access, authenticating, access rights, and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or workstation. It is a subset of computer security.

Network
A group of computers that communicate with each other.

Operating system
The program that manages all other programs in a computer.

Patch
An update to a computer program or system designed to fix a known problem or vulnerability.

Penetration test
A method of evaluating the security of a computer system or network by simulating an attack. The intent of a penetration test is to determine feasibility of an attack and the business impact of a successful exploit, if discovered.

Perimeter network
A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a perimeter network is to add another layer of security to an organization's local area network (LAN); an external attacker has direct access only to equipment in the perimeter network, rather than any other part of the network. Also known as a demilitarized zone.

Phishing
An attempt to obtain sensitive information, such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy organization in an electronic communication.

Physical access controls
The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

Ransomware
A type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Secure coding
The practice of developing application software in a way that reduces the risk of accidental introduction of security vulnerabilities in software before it is deployed.

Security event
An event in which an information system or a network has been breached or compromised, a security policy was violated, or a security safeguard failed.

Security vulnerability
A flaw, bug, or misconfiguration that can be exploited to gain unauthorized access to a network or information.

Security zone
An area within a network occupied by a group of systems and components with similar requirements for the protection of information and characteristics associated with those requirements. These shared requirements and characteristics will include a common data classification, including shared:

- data confidentiality and integrity requirements;
- access controls; and
- audit, logging, and monitoring requirements.

Server
A computer that hosts systems or data for use by other computers on a network. Typical computing servers are database servers, file servers, mail servers, print servers, web servers, gaming servers, and application servers.

Software
A set of machine-readable instructions that directs a computer to perform specific operations.

Standard operating environment
A standard implementation of an operating system and its associated software.

Threat
Anything that can exploit a vulnerability, intentionally or accidentally, and obtain access to, damage, or destroy an asset.

User access controls
The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights and requiring passwords.

Virtual private network (VPN)
A private network extended across a public network, such as the Internet. It enables a computer to send and receive data across a shared or public network as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network.

Web browser
A software program used by a computer to locate, retrieve, and display information from a website (such as Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome).

Workstation

A special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, it is commonly connected to a local area network and runs multi-user operating systems. Can also be anything from a mainframe computer terminal to a PC connected to a network.

Back to Table of Contents