Report 9: January 2013

SECURING THE JUSTIN SYSTEM: ACCESS AND SECURITY AUDIT AT THE MINISTRY OF JUSTICE

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250-419-6100
Facsimile: 250-387-1230
Website: www.bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2013 Report 9: *Securing the JUSTIN System - Access and Security Audit at the Ministry of Justice*, which was delayed until January 24 as per agreement with the Attorney General.

The audit reveals serious security flaws in JUSTIN, the Province's computerized criminal justice system, which supports the administration of criminal justice cases from initial submission through to the court process. Much of the information found in the JUSTIN database is highly sensitive. The audit concludes with more than 100 detailed recommendations that address JUSTIN deficiencies, many of which are too sensitive to include in this report.

In 2008, my office reported the results of an audit into the management of access to the Corrections Case Management System (CORNET), which also identified security flaws. The failure to apply recommendations from the CORNET audit to systems like JUSTIN leads me to question the quality of IT leadership and governance around criminal justice information.

John Doyle, MAcc, FCA
Auditor General

Victoria, British Columbia
January 2013

TABLE OF CONTENTS

AUDITOR GENERAL'S COMMENTS

John Doyle, MAcc, FCA
Auditor General

The Province maintains an integrated justice case management system, known as JUSTIN, to support the administration of criminal justice cases from initial police submissions to Crown assessments and through the court process. JUSTIN now contains over one million police investigations, including some of the most sensitive information held by government.

In the fall of 2011, my Office undertook an audit to review the protection of information in the JUSTIN system. We reviewed the security in place to detect and ward off attacks from the outside, and the controls to secure JUSTIN information from insider threats.

Effectively protecting this information is crucial to the privacy and personal safety of those involved. Given the sensitivity of the information, we expected to find layers of highly effective security controls at all potential access points.

Instead, our audit results revealed a serious lack of controls to protect JUSTIN information from inappropriate access, and virtually no controls for detecting or preventing unauthorized disclosure. Information in the JUSTIN system is not safe from motivated individuals looking to gain access to it, and equally concerning, there is very little chance that the ministry would ever know that unauthorized access had occurred.

This is not the first time I have reported serious concerns around the security of information in the criminal justice system. In 2008, I reported the results of an audit into the management of access to the Corrections Case Management System (CORNET). That audit also identified weak controls to prevent excessive internal access to sensitive information. The ministry was informed of the CORNET security issues four years before the audit of the JUSTIN system started, and now the same issues are being reported for a system that arguably contains even more sensitive information.

Had the recommendations from the CORNET audit been applied to other systems, the results of this audit would likely have been more positive. This failure to act, and the very fact that significant additional security weaknesses were allowed to exist at all, leads us to question the quality of IT leadership and governance around criminal justice information.

Underlying this report are 100 detailed recommendations for management to address the specific deficiencies. Many of the detailed issues covered are too sensitive to include in a public report. In publicly reporting the issues I have, I considered the risks to information security. I concluded that my report would not fundamentally alter the existing information security risk profile and that it is in the public interest that the report be published.

Although I have allowed the ministry additional time to address the recommendations, the Reports to Crown Counsel are not yet adequately protected. Serious security concerns still exist.

I would like to acknowledge the staff in the Ministry of Justice for the cooperation and assistance they provided to my staff during our work on this audit. My staff will continue monitoring the ministry’s progress toward protecting the JUSTIN environment.

John Doyle, MAcc, FCA
Auditor General of British Columbia

January 2013

AUDIT TEAM

Bill Gilhooly
Assistant Auditor General

Pam Hamilton
IT Audit Director

Ada Chiang
IT Audit Director

Joji Fortin
IT Audit Manager

JUSTIN IS A COMPUTERIZED system used across BC for managing and administering the criminal justice process. It allows adult and youth criminal cases to be tracked and processed from initial police arrests and Crown counsel charge assessments through to court judgement.

The JUSTIN database contains some of the most sensitive information in all of government, including Reports to Crown Counsel (RCCs), which contain details of police investigations, witness 'will say' statements, witness and victim contact information and charge assessments. JUSTIN information also includes accused history reports, law enforcement availability and court case tracking and administration.

While the availability of JUSTIN information is critical to the administration of justice in BC, disclosure of this information to the wrong people could compromise personal safety, and the integrity of the justice system. It is vitally important that JUSTIN user access is properly managed, with security controls in place to protect against inappropriate and unauthorized internal and external access.

Our audit examined how well JUSTIN information is protected from insider threats and external attacks. We looked at the risks posed by JUSTIN users and the controls in place that would detect and/or prevent unauthorized access and disclosure of information. To assess external threats, we conducted a series of penetration tests to try and reach critical resources on the network, and assessed the ability of the ministry to detect and prevent this type of threat.

CONCLUSION

- The information in the JUSTIN system is not adequately protected from internal or external threats.
- Controls in the JUSTIN system are inadequate to detect or prevent unauthorized access. It is unlikely that unauthorized access or removal of copied information will be discovered, and consequently risks from wrongful disclosure cannot be mitigated.

KEY RECOMMENDATIONS

We assessed the controls in place to protect JUSTIN information, and communicated our results to the Ministry of Justice throughout the audit. In July 2012, a detailed management report was provided to senior management. It documented our detailed findings and presented 100 recommendations, all of which were accepted by the ministry. We have summarized these into five overarching recommendations, in part to avoid introducing additional security risks.

We recommend:

1. 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.

2. User access to JUSTIN information should be granted and managed based on the principle of 'need to know'.

3. Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring in place.

4. More effective audit trails and tools should be in place to enable detection and investigation of suspicious or unauthorized activity.

5. An effective monitoring program should be in place to enable proactive detection of unauthorized access and removal of copied JUSTIN information.

Table 1: Number of detailed recommendations by audit area

Key audit area	Number of recommendations
User access to RCCs	18
System security	42
Application, database and user management	25
Incident detection and response	13
Security clearance	2
Total recommendations	**100**

The Ministry of Justice acknowledges the work carried out by the audit team during its thorough review of our JUSTIN application. The Auditor General has deferred issuance of the audit report in order to provide time to address the risks identified within this report. The security of the ministry's information systems is of paramount importance and the Ministry of Justice will continue to take proactive steps to ensure vigilant protection of sensitive data. The Ministry of Justice is committed to maintaining rigorous security of our information systems and has fully accepted the audit findings. The Ministry of Justice has taken immediate and appropriate actions to address the issues that have been raised and are implementing recommendations made within the report. The ministry would also like to acknowledge the efforts of the people, both inside and outside of the ministry who have been involved with the security of the JUSTIN application who have done a significant amount of work in a relatively short period of time to address the findings of this audit.

The penetration testing performed by the audit team found that the existing security controls were adequate to prevent direct attacks against JUSTIN from outside of the government network, but further observed that multiple layers of security are required to ensure a robust defence strategy. This report has identified several areas that are in need of improvement and the Ministry of Justice has responded by implementing measures to ensure heightened security of the JUSTIN system.

Throughout the audit process, Ministry of Justice staff worked closely with the audit team and took immediate action to address concerns as they were identified. The Ministry of Justice established a cross-government project team to oversee ongoing work related to improving JUSTIN security and will continue to meet regularly with the auditors to ensure an optimal understanding of the findings as recommendations are addressed.

The ministry must also acknowledge that while we accept the audit findings, in some cases the response diverges from specific recommendations provided by the auditors. As administrators of the JUSTIN system the Ministry must balance the need to restrict access to sensitive information with the need to enable the criminal justice system to effectively protect the citizens of British Columbia. The Ministry of Justice has taken steps to mitigate all immediate threats on a priority basis and has restricted access to the most sensitive information within JUSTIN while maintaining sufficient access for users to effectively perform their job duties. Additional improvements to the security of the information within JUSTIN will be achievable in time with enhancements to the JUSTIN application and its infrastructure. The Ministry recognizes that there are still outstanding gaps to be addressed however, all of the audit findings have now been thoroughly reviewed by the Ministry and immediate mitigations have been put in place to reduce identified risks. Furthermore, a multi-phased plan has been developed that will continue to close any gaps and will ultimately address all of the findings contained in this report.

The following actions are completed or underway and will directly enhance our ability to address the findings and recommendations:

1. JUSTIN access has been reviewed and users who no longer require access have had their permissions removed. Policies and procedures are being developed to ensure that staff changes are carefully monitored and access to JUSTIN is removed immediately when an employee changes jobs or no longer requires access. We have ensured that the security features in JUSTIN that should restrict access are applied properly to all active sensitive RCCs. A review of historical data and additional security features permitting more granular access are being analyzed for future inclusion as part of the ongoing review of the JUSTIN access model.

2. Network access has been reviewed and modified to remove access to any Justice systems by employees in other ministries unless a valid business need can be proven and approvals have been given. An ongoing review of network access will further strengthen security by verifying all network connections from Ministry of Justice offices to ensure they are valid. Remote accounts issued to regular government users are no longer able to access JUSTIN or other sensitive applications within the Ministry of Justice environment.

3. System administrators are now required to use a "Secure Access Gateway" to connect to any high-security Justice databases, including the JUSTIN database. There are no longer any direct connections from non-government computers and password policies have been updated for privileged operating system accounts.

4. JUSTIN system access is now being monitored to detect compromised accounts or inappropriate access: this will enhance our ability to detect anomalous system usage. Further enhancements to monitor user activity will be introduced with the enhanced security function under the ongoing project described below.

5. Training materials and guidelines have been updated to ensure that staff and partners are properly securing data within the system.

6. Criminal records checks are in place for all new employees who will have access to JUSTIN and contractors providing IT support for the system must now submit to more intense security screening.

Beyond the immediate mitigations, an ongoing project is addressing all areas of concern that have been identified. We are committed to the following actions and strategies:

1. Changes to the JUSTIN application access model will address concerns regarding access to RCC data by making it possible to establish more granular access. Ultimately, this will make it easier to ensure that the right people have access to the right information.

2. A move to new data centres in the coming months will ensure that the JUSTIN system is housed in a secure, state-of-the-art computing facility, with improved safeguards and better segregation between systems and environments.

3. A new, enhanced security function within the Ministry's Information System Branch will help refine and monitor security practices affecting information systems, including JUSTIN. This will include improvements to system monitoring and auditing capabilities, thereby greatly enhancing our ability to detect anomalous system usage or activity that could be indicative of inappropriate information access.

4. Ministry IT staff are working closely with central government IT services staff to improve the security of shared infrastructure services on which all ministries rely.

Approved By:

Richard J.M. Fyfe, QC
Deputy Attorney General

LWanamaker.

Lori Wanamaker, FCA
Deputy Solicitor General

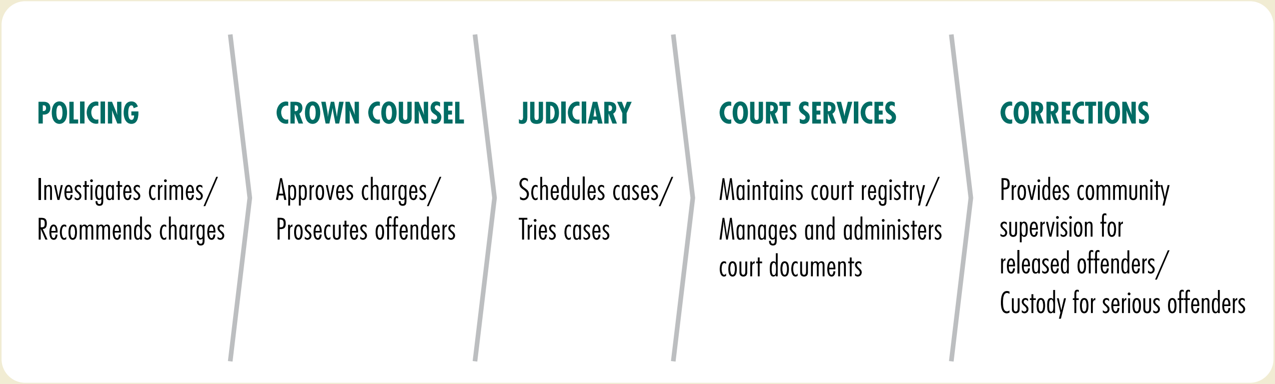
BACKGROUND

The JUSTIN system was fully implemented province-wide in 2001, and populated with Reports to Crown Counsel (RCCs) dating back to 1995, providing an integrated criminal justice system supported by a single provincial database for managing electronic court records.

The JUSTIN system is critical to the administration of justice in BC as it facilitates key components: RCC charge information, accused history reporting, court case tracking, court administration, witness notification and offence management information for use by police, Judiciary, Criminal Justice Branch, Court Services Branch and Corrections Branch staff.

Case information in the form of RCCs is first submitted to JUSTIN from the police system, PRIME-BC. RCCs are filled out during police investigations and used by the Crown Counsel to determine if charges will be laid. Once charges are approved, cases are scheduled through the courts. Depending on the decisions reached, Corrections may provide supervision over offenders, either in the community or in custody. An overview of the criminal justice process flow is shown in Exhibit 1.

Exhibit 1: Criminal justice process flow



POLICING

Investigates crimes/
Recommends charges

CROWN COUNSEL

Approves charges/
Prosecutes offenders

JUDICIARY

Schedules cases/
Tries cases

COURT SERVICES

Maintains court registry/
Manages and administers
court documents

CORRECTIONS

Provides community
supervision for
released offenders/
Custody for serious offenders

Source: Ministry of Finance, modified by the Office of the Auditor General

JUSTIN is jointly managed by the Ministry of Justice, the Judiciary and representatives of stakeholder groups including: the Royal Canadian Mounted Police (RCMP), the Federal Department of Justice and the Ministry of Children and Family Development.

There are over 3,300 JUSTIN users with RCC access at all levels of government: provincial, federal and municipal. The JUSTIN user population is spread over hundreds of locations throughout BC, including over 200 provincial and federal sites, 15 municipal police agencies, and over 150 RCMP detachments.

JUSTIN APPLICATION

The JUSTIN application is comprised of a suite of modules that follows the operational workflow of the criminal justice process. The main modules include the following:

- **RCC Module** - used by the police for submission of investigations in the form of RCCs and by ministry users for security assessments and other analysis;
- **Crown Module** - accesses the RCC and is used by Crown Counsel for charge assessments;
- **Courts Module** - used for preparing documents and tracking cases through the court system;
- **Trial Scheduling Module** - used for scheduling courtrooms, judges, police officers and Crown witnesses;
- **Law Enforcement Availability Module** - used by the police, Crown and corrections personnel to enter their availability for trial scheduling purposes; and the
- **Justice Administration System Module** - used by support staff for data administration, housekeeping and data quality purposes.

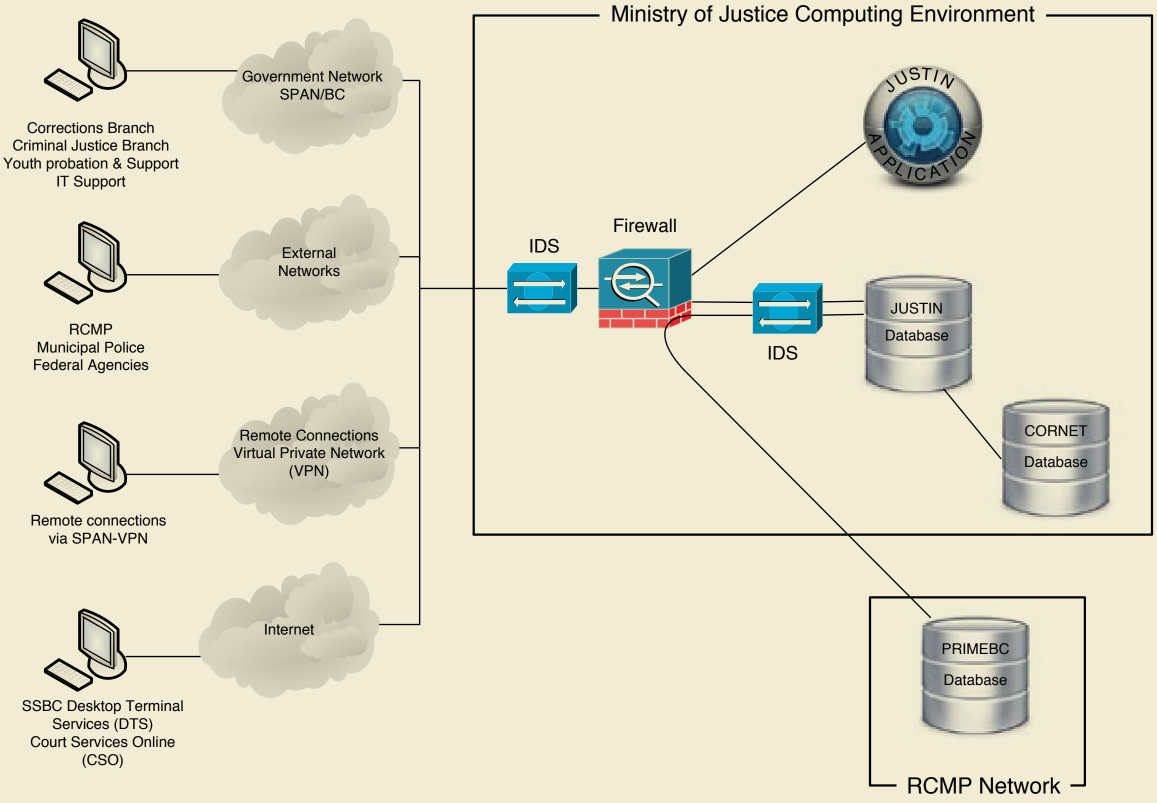
Our audit assessed access to RCC information via the RCC and Crown modules.

COMPUTING ENVIRONMENT

JUSTIN is a custom coded, web-based application running on a Solaris operating system, using an Oracle database. It is physically located in two data centres supported by multiple organizations. Users pass through the Ministry of Justice firewall to communicate with the JUSTIN application, which in turn, is firewalled again before communicating with the database. There are Intrusion Detection Systems (IDS) to provide additional traffic monitoring at key entry points.

A simplified overview of the JUSTIN computing environment is shown below in Exhibit 2.

Exhibit 2: A simplified view of the JUSTIN computing environment



Source: Ministry of Finance, modified by the Office of the Auditor General

AUDIT OBJECTIVES AND SCOPE

The main objective of the audit was to assess whether the JUSTIN system is effectively managed to protect against unauthorized access to information in the system. To determine this, we assessed whether:

1. The system is adequately secured from internal and external threats.

2. JUSTIN information breaches are likely to be discovered and effectively managed.

The audit focused on the protection of JUSTIN information by examining user access and the presence and adequacy of controls at key entry points to the JUSTIN system – the network, the operating system, the Oracle database and the JUSTIN application.

The detailed section of this report is grouped into six main audit areas:

Audit Area	What We Did
Penetration testing	Assessed the strength of the controls in detecting and preventing intrusion through simulated attacks
User access to RCCs	Assessed the threat of unauthorized disclosure of JUSTIN information by examining user access
System Security	Assessed the state of security by evaluating the existence and adequacy of network and system controls
Application, database, and account management	Assessed the risk of unauthorized access to JUSTIN by examining the management of user access, database roles and links, accounts and passwords
Incident detection and response	Assessed the ability to detect and respond to unauthorized access that could lead to wrongful disclosure of information
Security clearance	Assessed the extent to which criminal record checks have been a requirement for JUSTIN users

Our audit objectives and criteria were based on international standards issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC): ISO/IEC 27002 on Information Technology – Security Techniques – Code of Practice for Information Security Management.

We conducted this work under the authority of section 11(8) of the Auditor General Act in accordance with assurance standards established by the Canadian Institute of Chartered Accountants. A snapshot of the JUSTIN database, extracted on August 22, 2011, was used in the examination. The examination was carried out during the period from October 2011 to April 2012.

KEY FINDINGS

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

PENETRATION TESTING

Penetration testing is a method of exploiting the vulnerabilities within a system in order to gain access to critical data, simulating what an attacker would do. The results expose possible security weaknesses in a system as well as test its ability to detect and prevent attacks. A successful penetration test does not indicate that an attacker has previously broken in, however, it does reveal weaknesses in the system. Conversely, an unsuccessful penetration test does not necessarily mean that the system is safe from attacks, as there are many possible paths into a system, all of which cannot reasonably be scoped into a penetration testing schedule.

Penetration testing approach

We performed penetration testing using the services of an industry expert. We attempted to gain access via the Internet with no access privileges, and again from a slightly more privileged position via government network access.

Findings

- Tests were performed against the publically available Court Services Online via the Internet and against the JUSTIN application and other resources accessible via government network access. Security controls in the Court Services Online system, which has access to the JUSTIN database were tested. It appears that the controls are sufficient in preventing successful attacks initiated from the Internet.

- The security controls implemented to protect the JUSTIN application were tested and found to be adequate in preventing a direct attack via the government network.

- Our testing included scanning parts of the Ministry of Justice environment for the general availability of systems. From the scans, we were able to gain access to other systems that contained highly sensitive JUSTIN information, and other information which could be used to initiate further attacks on additional systems.

- Our testing also included assessing the controls in place to detect or stop an attacker. The controls were inadequate in detecting our presence and would not prevent the removal of copied information from compromised systems.

USER ACCESS TO RCCS

"Need-to-know" is a fundamental security principle in designing and applying access to information in IT systems. This is especially important in cases where the information being protected is sensitive, as with JUSTIN. Applying this principle effectively means assigning and managing access based on what each user needs on a routine basis to perform his or her duties.

Findings

- The "Need-to-know" principle has not been the foundation for determining access, nor has the JUSTIN application been configured to allow for applying this principle. Consequently over 3,300 users have broad access to RCCs, beyond what is required for performing their duties.
- The roles allowing user access to RCCs are not configured in a way that restricts users to specific parts of them. All users with RCC access have access to the entire RCC.
- Security features that should restrict access are not applied properly, allowing users excessive and inappropriate access, and the unrestricted capability to print and save RCC information to external devices.
- There are no guidelines to classify data based on its level of sensitivity, resulting in highly sensitive data being generally available to users. This includes RCCs pertaining to provincial and federal cases, and RCCs involving youth, pardoned individuals and sealed court cases.
- Access is not effectively monitored to promptly remove it when users change positions or employment status.
- Access to copies of the production database is excessive. A number of users have full, unmonitored access to the entire JUSTIN database, including IT support, researchers and some business users.

SYSTEM SECURITY

One of the main benefits of computer networks is that they enable users to access and use system resources, such as entries or searches into databases, from many local and remote locations. However, if the network is not properly secured and managed, significant inappropriate or malicious access to critical resources can occur.

Multiple layers of security, a "defence-in-depth" approach throughout the network, will provide improved security, and guard against exposure due to the failure of a single security component, software flaws or configuration mistakes.

Findings

- The Ministry of Justice firewall allows thousands of government network users to reach the JUSTIN system, regardless of whether or not they are authorized to use JUSTIN. This access is excessive and inappropriate. The JUSTIN system is running on servers that are not properly secured.
- Unsecured computers are able to connect directly to the JUSTIN database.
- Remote accounts issued to regular government users are able to reach critical resources within the Ministry of Justice environment.
- Vendor updates to fix critical security issues are not applied to system components.
- Non-production environments, which are typically less secure, are not segregated from the production environment.

APPLICATION, DATABASE AND USER MANAGEMENT

The overall strength of security in a system is also dependent on key design decisions, and the implementation of business processes to support them. For example, a framework for determining user access based on business needs is a basis for establishing appropriate user access. Procedures for managing user accounts, rules for setting passwords and guidelines for direct connections to the database are fundamental and provide a foundation for creating a secure computing environment.

Findings

- There is no pre-defined set of rules defining the access that JUSTIN users and support staff should have, based on their duties and business requirements.
- Downloads via direct connections to the JUSTIN database could be made without detection.
- Activity via direct connections to the JUSTIN database are not recorded or monitored.
- Connections to JUSTIN using non-government computers can be made directly to the production database.
- IT support staff have unlimited, unmonitored access to all JUSTIN information.
- Access through the operating system to the database is unmonitored.
- Accounts are not disabled promptly when users' employment ends or changes.
- There is evidence of account sharing in the audit trails. No detection or prevention methods are deployed to prevent account sharing or identify compromised accounts.
- Unsecure password practices are being used for privileged operating system accounts.

INCIDENT DETECTION AND RESPONSE

Prompt and appropriate response to unauthorized accesses is only possible if adequate detection methods are in place and actively used to identify suspicious activity. This includes extensive logging and regular monitoring of system activity. Detection methods also include the use of specialized tools such as intrusion detection systems and database content monitoring software that can identify internal and external threats and attacks.

Findings

- There is insufficient user activity information collected to allow for proper detection or investigation of unauthorized accesses.
- Audit trails are not regularly monitored to detect unauthorized or suspicious activity.
- There are no content monitoring tools deployed, at either the database or application level, that would detect threats and enable early alerting.
- Downloads made via direct accesses to the JUSTIN database are not logged, leaving no trail for analysis of access activity.
- Monitoring is not effectively detecting unauthorized activity. Several incidents have been brought to government's attention where parties involved in legal cases became aware that their case information had been inappropriately disclosed. These disclosures were the result of misuse of JUSTIN access privileges.

SCREENING

Criminal record checks can assist in identifying people with criminal backgrounds that should not be given access to JUSTIN.

Findings

- 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.

APPENDIX A: GLOSSARY

CORNET: CORNET refers to the Corrections Network System. It is an offender information and case management system for both adult and youth offenders in provincial corrections programs.

Court Services Online: Court Services Online is an electronic service, accessible from the Internet, allowing public viewing of court files, daily court lists and electronic filing of civil documents. It interacts with the user via a web front-end, displaying information from JUSTIN based on user requests.

Database: A database is a collection of information organized in such a way that a computer program can quickly select desired pieces of data. You can think of a database as an electronic filing system. (Source: www.webopedia.com)

Database roles: Database roles allow access to be indirectly assigned to users. By using roles, users do not have to be given direct access to data. Tables, views, procedures and other database objects are assigned to roles and roles are assigned to users. Roles are generally assigned many more tables than each user needs, but through the application controls the users will be limited to only the information they are authorized to access.

Firewall: A firewall is designed to prevent unauthorized access to, or from, a network. It can be hardware, software, or a combination of both. All messages entering or leaving the network through the firewall are examined and those that do not meet the specified security criteria are blocked. (Source: www.webopedia.com)

Intrusion detection system: An intrusion detection system (IDS) inspects and alerts on inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system and its resources. (Source: www.webopedia.com)

Operating system: An operating system is the program that manages all other programs in the computer. Other programs make use of the operating system by making requests for services. Users can also interact directly with the operating system.

Penetration test: A penetration test is 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. (Source: www.wikipedia.org)

PRIME-BC: PRIME-BC refers to the Police Records Information Management Environment for British Columbia system that connects every municipal department and RCMP detachment throughout the province. It provides police agencies access to information about criminals and crimes instantly. (Source: www.bc.rcmp.ca)

Virtual Private Network (VPN): A VPN, or virtual private network, is a network that is constructed by using public wires to connect nodes. There are a number of systems that enable creation of networks using the Internet as the medium for transporting data. Encryption and other security mechanisms are used to ensure that only authorized users can access the network and that the data cannot be intercepted or altered. (Source: www.webopedia.com)

OFFICE OF THE
Auditor General
of British Columbia

Location:

8 Bastion Square
Victoria, British Columbia
V8V 1X4

Office Hours:

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll free through Enquiry BC at: 1-800-663-7867
In Vancouver dial 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website:

This report and others are available at our website, which also contains further information about the office: www.bcauditor.com

Reproducing: