SECURITY INTELLIGENCE REVIEW COMMITTEE

TOP SECRET – CEO

SIRC REVIEW 2013-06
THE INSIDER THREAT AND ITS EFFECT ON INFORMATION MANAGEMENT

SUMMARY

This review set out to examine the Service's efforts at preventing insider threats, especially as it relates to information management, given the increased magnitude of this threat in the post-Delisle, post-Snowden era. The review observed that CSIS has taken its obligations to allied agencies quite seriously, particularly with respect to meeting requirements for shared security initiatives. In addition, SIRC found that CSIS is addressing the insider threat problem in its practices and policies: the Service administers its physical security (including search policies) with the expected level of attention, it has leveraged its expertise to foster measurable improvements concerning IT security, and CSIS has streamlined security checks during its hiring process.

SUMMARY OF RECOMMENDATIONS

- SIRC recommended that CSIS immediately develop robust procedures governing Access Lists.
- SIRC recommended that CSIS re-examine an internal investigation file in its entirety, and that six specific concerns

- SIRC recommended that CSIS create a robust training and mentoring program suited to the unique work of Internal Security employees.
- SIRC recommended that CSIS create more detailed policy on the conduct of Internal Security investigations into suspected violations and/or breaches of security.
- SIRC recommended that CSIS take immediate action to ensure that all decision-making pertaining to internal investigations be documented within the appropriate case file, in accordance with the standard requirements set by Treasury Board guidelines.
- SIRC recommended that upon completing a Formal Investigation, Internal Security should forward the final investigation report to a group outside Internal Security for review, prior to it being provided to the Director.

File No. 2800-183 (TD R537)

Table of Contents

1 INTRODUCTION

The 9/11 attacks led to a paradigm shift in information management among intelligence agencies: information stovepipes were eradicated, leading to over a decade of unprecedented sharing. The conventional wisdom which emerged from this decade – that broad sharing among allies provides a net benefit – has been increasingly challenged by a number of security breaches within Western intelligence and military services. In 2010, WikiLeaks publically embarrassed the American government by releasing thousands of classified documents, and by the same stroke shed public attention on Canadian intelligence practices.[1] Likewise, the espionage of former Sub-Lt Jeffrey Paul Delisle caused serious injury to both Canada's national interests, as well as those of close allied nations Finally, the case of Edward Snowden has highlighted that the damage resulting from a security breach is seldom contained to a single agency.

The entire Five Eyes community has appropriately elevated the concern posed by the insider threat – described by CSIS as "any person with authorized access who causes harm, intentionally or otherwise, to the assets of the organization (employee, contractor)" – to the highest levels in order to reduce its rate of occurrence, and failing that, to help limit the damage that can be caused by a malicious internal actor. This review, therefore, set out to examine the Service's efforts at preventing insider threats, especially as it relates to information management.

The review observed that CSIS has taken its obligations to allied agencies quite seriously, particularly with respect to meeting requirements for shared security initiatives. Additionally, CSIS has supported the needs of Canadian agencies and departments who are not as experienced in security matters, and worked on numerous internal measures aimed at improving the security of Service assets and employees.

That said, the review did find a number of serious shortcomings related to CSIS's handling of sensitive case files, as well as to the current practices and management of internal investigations; in one case, these failings led the Committee to recommend that CSIS thoroughly re-examine an internal investigation.

Given the gravity of these findings, SIRC made a number of comprehensive recommendations aimed at improving policies, investigative thresholds, and documentation procedures. These recommendations are further supported by the Committees' final recommendation that, in the future, an independent assessment of all CSIS internal investigations should be reviewed by an objective third party outside of Internal Security to help ensure that the investigation is complete, objective and well-documented.

[1] "CSIS 'vigorously harassing' Hezbollah, got help from Iran: U.S. cable," Toronto Star, November 29, 2010.

Finally, in light of the serious issues noted, SIRC intends to examine CSIS's internal security activities on an annual basis. The purpose of this undertaking is to evaluate whether internal investigations and other security processes, including the management of sensitive case files, meet with the stringent security practices expected of a modern intelligence agency.

2 METHODOLOGY

This study included an extensive review of documentation, such as CSIS internal policies and procedures, planning and discussion papers, internal audits and records of violations and breaches, injury assessments, records of correspondence with foreign and domestic partners working on joint security initiatives, and documentation pertaining to initiatives impacting internal security. SIRC also examined various matrixes used for security-related issues at CSIS, as well as a number of internal investigations into suspected violations and/or breaches of security. Further to this documentation review, SIRC submitted a number of written questions to CSIS to assist in clarifying its understanding of decisions and/or incidents, or in providing additional context.

SIRC met with a number of CSIS representatives to both provide context to the issues under review, as well as to receive updates on ongoing security initiatives. The discussions included meetings with Internal Security (IS) Branch, Information Management & Information Technology (IM/IT) Branch, Human Resources (HR) Branch, and finally, two meetings with investigators within

The review period covered January 1, 2010 to May 1, 2013, although a considerable amount of information was received from outside this period in order to allow the Committee to adequately assess a number of important issues and developments that fell within the scope of the review.

3 SECURITY STANDARDS

Events of recent years have underscored the serious fallout that can result from security breaches In particular, the technological ability to remove and alter unprecedented amounts of information from otherwise secure buildings (e.g. through USB keys),

Page

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information Act

de la Loi sur l'accès à l'information

4 CSIS'S INTERNAL SECURITY BRANCH

CSIS itself has undertaken a number of measures to augment security practices and procedures in an effort to address the insider threat. In many respects, the lynchpin to the maintenance of CSIS's protection against insider threats is the IS Branch. The responsibilities of IS are vast, including offering technological security guidance giving general security advice to employees outlining rules governing mandatory polygraph examinations, physical searches and security 'spot checks', and numerous other activities aimed at "managing the development and implementation of the national security program to protect CSIS, its assets, operations and employees from all security threats."[14]

SIRC singled out four areas for in-depth examination, discussed separately below:

- security-based hiring/recruiting procedures;
- physical security of CSIS facilities including entry/exit spot checks;
- access lists restricting viewership and/or knowledge of sensitive files; and,
- internal investigation of suspected security violations/breaches (reviewed in the following section).

4.1 Employee Hiring

Former CSEC Chief John Adams noted that "the worst threat is the insider threat...you've got to be sure (that new employees) are clean when they come in and they stay that way when they're there."[15] In carrying out its review, SIRC noted that CSIS's hiring process has recently undergone significant change,

a process that involves not only multiple interviews, but background security checks, suitability questionnaires, management vetting, a psychological profile and a polygraph test.

[15] Murray Brewster and Jim Bronskill, "U.S. looking over Canadian military's shoulder in wake of navy spy scandal: sources," National Post, May 27, 2013.

4.2 Physical Security

Physical security, most notably the ability to monitor what is brought in or taken out of CSIS's premises, is of crucial importance in a secure environment.

SIRC examined a range of documentation pertaining to the enforcement of physical security and the tracking of violations.

Overall, **SIRC found that CSIS addresses its physical security with the expected level of attention, and reacted appropriately to the violations which took place at its facilities.** Of note, during the review period, there was a concerted effort to address some employee concerns regarding the legal foundations of CSIS's search policies;

4.3 Access Lists

Like any organization that must keep track of how sensitive information is accessed and by whom, CSIS employs what are commonly referred to as a Access Lists: literally, a list of names of individuals who have been exposed to a particularly sensitive file's contents. Access to a file is not fixed: indeed, the sensitivity of a file evolves depending on the stage of the investigation and the ultimate conclusion of the file. For this reason, Access Lists are one tool among many which help to control access to sensitive files. That said, SIRC has been told on numerous occasions of the importance of Access Lists to the security of a file.

Given all of the above, **SIRC found multiple examples of a haphazard application of access standards to files which the Service considered highly sensitive, as well as a lack of documented procedures governing the functioning and maintenance of its Access Lists.**

4.4 Developing Policy and Procedures Governing Access Lists

In the post-Snowden era, the ability to control and retroactively audit access to sensitive and classified information has become a standard expectation of the entire Five Eyes community. After careful consideration and study, SIRC believes that a proper Access List regime should include the following:

SIRC recommends that CSIS immediately develop robust procedures governing Access Lists.

5 INTERNAL INVESTIGATIONS

The protection of the Service's employees, information and infrastructure from compromise is fundamental to CSIS's ability to fulfil its mandate. When a suspected security violation or breach of security occurs,[31] CSIS will conduct internal security investigations that may range from Fact-Finding Inquiries, up to Formal Investigations or Administrative Reviews.[32]

SIRC received a synopsis of all internal investigations regarding actual or suspected security threats, breaches or violations between 2007 and 2013.

Given the wide range of cases to choose from, SIRC initially selected files spanning multiple years, and chose an additional investigation given the context it provided to the other files already being examined.

All internal investigations are conducted by IS personnel, and according to CSIS policy, these investigations "will be thorough, fair, and will be in accordance with the CSIS Procedures: Breaches of Conduct and Disciplinary Measures." SIRC therefore used these policies and guidelines to help understand how internal investigations were *expected* to proceed, and used these standards to assess how investigations *actually* progressed. After its review, SIRC identified three interrelated issues.

First, SIRC found that there was insufficient training, gaps in policy and procedures, and a lack of managerial feedback for employees working on internal investigations. There is a significant difference between the work of an Intelligence Officer (IO) collecting information on national security threats and that of an IS employee conducting an internal investigation on breaches of security by *colleagues*. There is no comprehensive CSIS mentoring program or training to address the unique challenges of investigating former and future colleagues, subordinates and supervisors, all with similar background, training and experience.

---

[31] A security violation is any contravention of Service security policy or procedures. Usually, violations of security are omissions or acts which could cause the unauthorized disclosure of -- or access to -- classified or designated information or assets. This includes any contravention of the need to know principle. A breach of security occurs when any classified or designated information or asset is the subject of unauthorized access or disclosure. This may include unauthorized disclosure by any person, or theft, loss or exposure in circumstances that make it probable that unauthorized access or disclosure has occurred.

[32] Fact Finding Inquiry: Usually the discovery stage of an investigation into an alleged breach or violation of security, or a security incident, wherein the facts are ascertained in order to determine whether the allegation is substantiated, and whether a formal investigation is warranted; Formal Investigation: An administrative investigation which proceeds under the authority of approved terms of reference; Administrative Review: A fact-finding inquiry requested by the Director, further to a serious security incident, which may include the interview of employees and any other measures as determined by the Director. Any potential conduct issues must be referred to a formal investigation.

Additionally, SIRC noted that policy and procedures governing internal investigations (certainly prior to recent updates),[37] have been unclear and unsystematic.

Second, SIRC found that there are unsatisfactory thresholds for internal investigations. Although IS can conduct a number of activities ranging from fact-finding inquiries to formal investigations, the threshold whereby a suspected breach or violation moves from a "fact finding" assignment to an official investigation is unclear and appears subjective, even when taking into account recent policy updates.

Refined definitions involving fact-finding and formal investigations have been created with the issuance of new policy, but the parameters, guidelines and timelines to assist in determining when to elevate issues to formal investigations continue to lack objective standards.

Third, SIRC found that CSIS did not maintain proper documentation on decision-making surrounding internal investigations.

Page

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information Act

de la Loi sur l'accès à l'information

Page

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information Act

de la Loi sur l'accès à l'information

Page

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information Act

de la Loi sur l'accès à l'information

Page

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information Act

de la Loi sur l'accès à l'information

As a result, **SIRC recommends that CSIS re-examine the in its entirety, with the following six concerns**

Page 492

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information Act

de la Loi sur l'accès à l'information

7 THE WAY FORWARD – RECOMMENDED CHANGES TO INTERNAL INVESTIGATION PRACTICES

SIRC believes that a number of changes must be undertaken to improve the conduct and management of internal investigations. **Therefore, SIRC recommends**:

1. **That CSIS create a robust training and mentoring program suited to the unique work of Internal Security employees who are expected to conduct sensitive investigations into suspected violations and/or breaches of security. This training should be complemented by appropriate and precise guidelines, such as would be elucidated in a procedural manual;**

2. **That CSIS create more detailed policy on the conduct of Internal Security investigations into suspected violations and/or breaches of security. This policy should clearly stipulate the thresholds to be used when making determinations on issues such as the required level of investigation and the thresholds involved in the use of specific tools and techniques; and,**

3. **That CSIS take immediate action to ensure that all decision-making pertaining to internal investigations be documented within the appropriate case file, in accordance with the standard requirements set by Treasury Board guidelines.**

SIRC believes that these improvements are necessary for the internal investigations process to achieve its expected level of professionalism and rigour.

SIRC believes there is a value in having a second set of eyes reviewing the results of internal investigations. Indeed, SIRC is concerned about the appropriateness of having solely IS employees conduct investigations without any further checks and balances ensuring the reasonableness and appropriateness of the decisions being rendered, given the potential gravity of their consequences. For these reasons, SIRC believes that further internal safeguards are necessary. **Specifically, SIRC recommends that upon completing a Formal Investigation, Internal Security should forward the final investigation report to a group outside Internal Security for review, prior to it**

being provided to the Director.

SIRC believes that this additional quality control process will assist the Director in making an appropriate determination on the reasonableness of the investigation's findings. In light of its findings, SIRC intends to regularly review internal security activities:

8 CONCLUSION

SIRC's review set out to evaluate CSIS's response to the Insider Threat, particularly as it relates to information management. Along the way, SIRC found that CSIS was committed to fully implementing the guidelines

APPENDIX A: FINDINGS

SIRC found that following implementation of the there was a noted decrease in the number of IT violations at CSIS.

SIRC found that CSIS addresses its physical security with the expected level of attention, and reacted appropriately to the violations which took place at its facilities.

SIRC found that there was insufficient training, gaps in policy and procedures, and a lack of managerial feedback for employees working on internal investigations.

SIRC found that there are unsatisfactory thresholds for internal investigations.

SIRC found that CSIS did not maintain proper documentation on decision-making surrounding internal investigations.

APPENDIX B: RECOMMENDATIONS

SIRC recommends that CSIS immediately develop robust procedures governing Access Lists.

SIRC recommends that CSIS re-examine file in its entirety, and that the following six concerns

SIRC recommends that CSIS create a robust training and mentoring program suited to the unique work of Internal Security employees who are expected to conduct sensitive investigations into suspected violations and/or breaches of security. This training should be complemented by appropriate and precise guidelines, such as would be elucidated in a procedural manual.

SIRC recommends that CSIS create more detailed policy on the conduct of Internal Security investigations into suspected violations and/or breaches of security. This policy should clearly stipulate the thresholds to be used when making determinations on issues such as the required level of investigation, and the thresholds involved in the use of specific tools and techniques.

SIRC recommends that CSIS take immediate action to ensure that all decision-making pertaining to internal investigations be documented within the appropriate case file, in accordance with the standard requirements set by Treasury Board guidelines.

SIRC recommends that upon completing a Formal Investigation, Internal Security should forward the final investigation report to a group outside Internal Security for review, prior to it being provided to the Director.