

## Information Protection Centre Executive Security Report Q1-2010/11

### Introduction

The IPC executive security report provides a quarterly summary of key security metrics including commentary, analysis and recommendations where appropriate. The report provides information and metrics gathered from a variety of security technologies used to protect the government network for the first quarter of 2010/11.

### Internet Junk Email (SPAM) Statistics

Monthly Totals	April - 2010	May - 2010	June - 2010
Attempted Deliveries (Before Filtering in Millions)	110.37	118.11	112.88
Actual Email Delivered to Staff (Millions)	2.62 (2%)	2.54 (2%)	2.51 (2%)
<b>Actions</b>			
Blocked (Millions)	101.7 (97%)	114.74 (97%)	109.63 (97%)
Viruses	239	333	348
Quarantined for review by the Recipient	0.84%	0.71%	0.65%
Tagged (Spam Warning included with the Message)	0.05%	0.04%	0.04%
White listed	0.16%	0.13%	0.13%
Attachments Discarded (On GOM Block List)	718	858	1514

Virus Statistics	Q1 - 2010 (April - June)
Web Browsing	618 (New)
GOM Application Servers	0
HP File/Print Servers	71
HP Exchange Email Servers	58
Desktop Computers	1994
Internet Email	920
<b>Total Number of Viruses:</b>	<b>3661</b>

### Internet Junk Email & Virus Analysis

The government perimeter email service that provides the junk email (SPAM) filtering provides a highly reliable anti spam service. Junk email volume varies from month to month with the amount of actual email delivered to staff remaining consistent at approximately 2.5 million messages per month. These numbers are consistent with the fourth quarter of 2009/10 where on average 2-3 percent of all email was legitimate with the rest being junk email. The virus statistics related to SPAM and Internet email are artificially low because government currently blocks over fifty major attachment types deemed to be unsafe.

### Update from Q4 2009 Report

In the fourth quarter report of 2009 the IPC reported that the existing web browsing antivirus solution provided by ██████ had become ineffective. During the first quarter of 2010/11 the IPC and IMS replaced the ██████ web browsing antivirus solution leveraging the existing proxy service from ██████ and antivirus from ██████. This introduces a second antivirus technology to the environment in addition to the corporate standard ██████ providing an additional layer of defense.

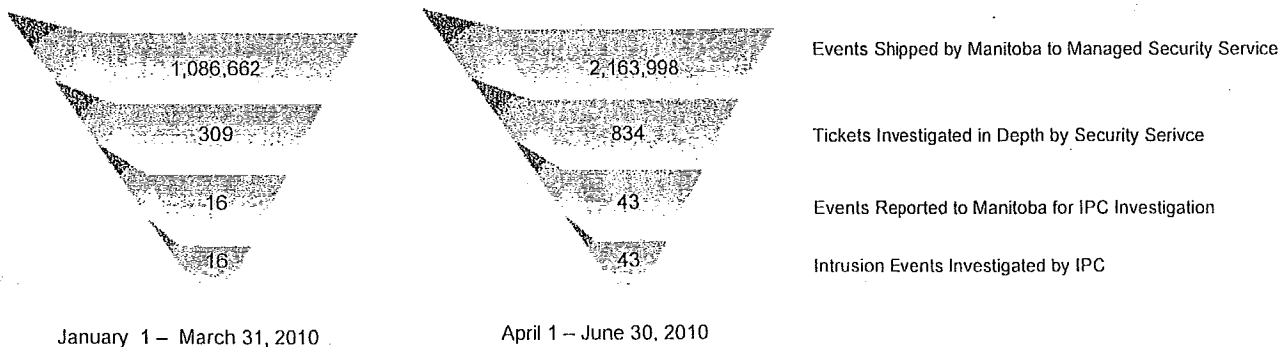
During the fourth quarter the IPC reported that preliminary investigations were underway on implementing offline web content filtering and web reputation services. Web Reputation Services block access to web sites that have been compromised and are updated real time by the web reputation service provider. The service works both in and outside the managed environment allowing BTT to protect laptops that are working out of the office. The Web Reputation Service is included in the government's corporate antivirus license. Preliminary estimates provided by [REDACTED] to implement the web reputation were rejected by IPC and IMS. The IPC demonstrated that the level of effort to implement the web reputation service is minimal and [REDACTED] is revising the cost estimates at this time.

Due to conflicting work loads of [REDACTED] IMS and IPC no progress to date has been made in implementing offline content filtering. Mobile computers are extremely susceptible to viruses when disconnected from the government network because they do not receive the protection provided by the government Internet service that blocks viruses and restricts users from visiting sites forbidden in the *Employee Network Usage Policy (ENUP)*. Enhancements to the current technology used by government will allow for offline content filtering that will enforce the same policies on users when they are disconnected from the network and working away from the office. IMS and IPC plan to pursue this option and continue to research how the technology works and how it would be implemented in government.

### Intrusion Detection Statistics

The government has an extensive network of intrusion detection and intrusion prevention technology monitoring the network. Prevention devices actively block malicious attacks while the detection technology simply monitors and reports. The IDS/IPS technology is one of the primary security technologies used by the IPC with 24x7 support provided by [REDACTED]. The 24x7 service has been monitoring the government since September 2009. Events are shipped to [REDACTED] who triage and report major events to IPC for incident response. Figure 1 below shows the process used to filter events and the value of outsourcing this specialty to a managed service provider.

Figure 1



Events reported to the IPC by [REDACTED] are investigated to determine the potential impacts on government. Some events are violation of government policy, while other events include hacking attempts on government assets. The IPC continues to work with [REDACTED] to refine the number of events reported. The number of events investigated by IPC was higher than normal due to a number of incidents with public access workstations. These events are detected by the security service but do not pose a security threat to the government because of the compensating controls surrounding public access workstations that isolates them from the government network. The number of overall events shipped by Manitoba to the Managed Security Services jumped overall because of ongoing efforts to tune the intrusion detection devices to optimize the reporting and an overall increase in intrusion activity on the Internet.

### **Security Awareness**

The Information Security Awareness training program was developed in response to recommendations from the Office of the Auditor General. Since its launch in 2006 the IPC has trained approximately 5000 civil servants. The IPC has conducted twelve awareness sessions this quarter with 175 attendees. The IPC has completed development of an electronic learning (eLearning) version of the training. The eLearning program will be delivered through the Organization and Staff Development (OSD) learning management system and will be ready to launch with the electronic version of the corporate orientation program. Discussions are underway with the Civil Service Commission on mandatory participation in the corporate orientation program and the security awareness program during a new hires probation period.

### **Forensic Investigations**

The IPC conducts ICT forensic investigations in support of Human Resources. All forensic investigations are approved in advance by Labour Relations. The IPC conducted eight employee forensic investigations during the first quarter of 2010/11. The number of investigations is tracking similar to 2009 when the IPC conducted a total of 42 employee forensic investigations.

### **Application Security Assessments**

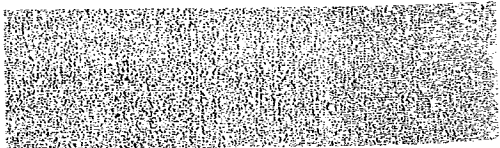
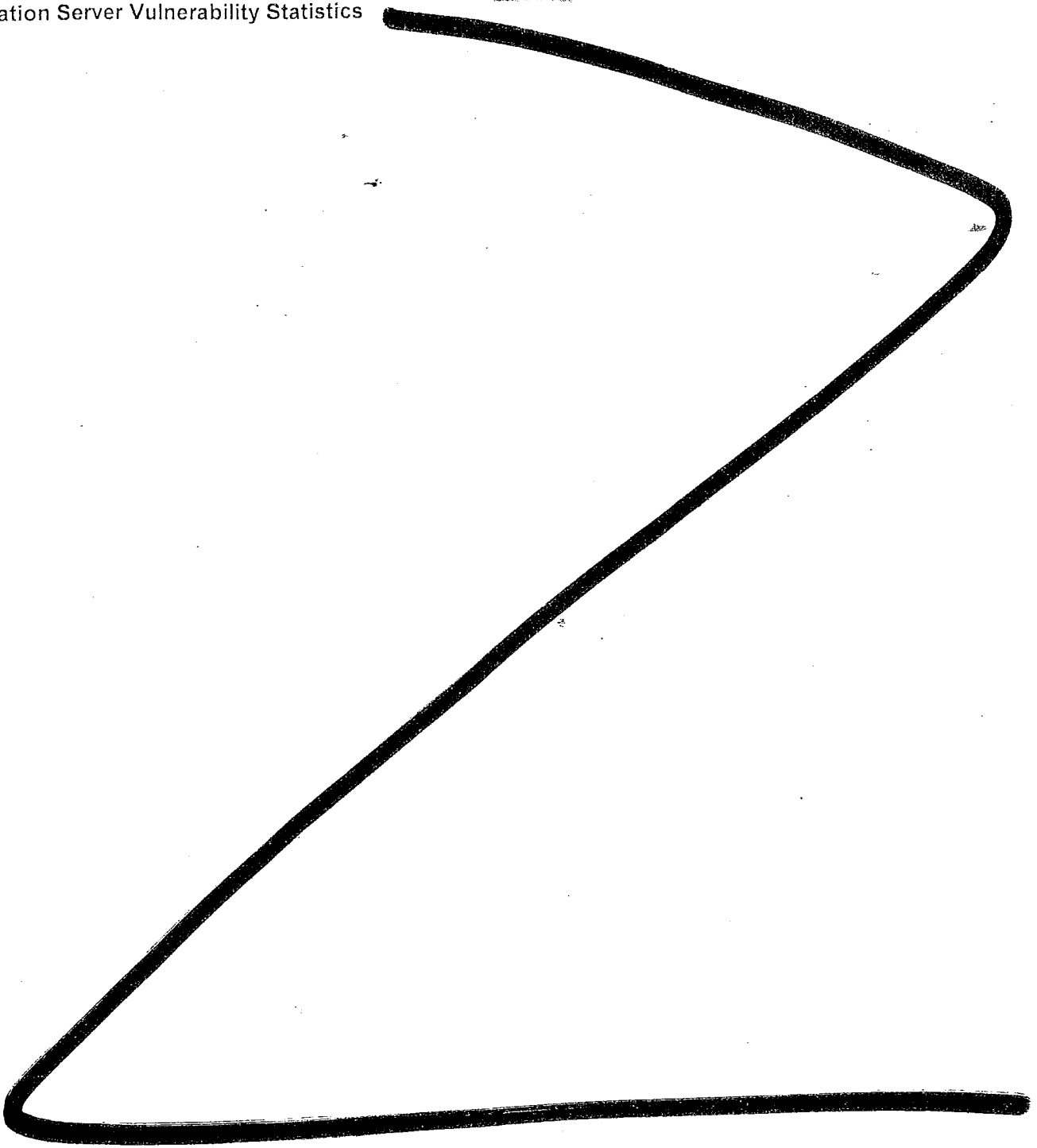
The IPC conducts security assessments of new solution architectures and in depth application assessments of the final developed solution and hosting environments prior to going live. This includes both common off the shelf software and custom software including software developed by contractors. The IPC conducted 10 reviews of both solution architectures and production applications prior to going live during the first quarter of 2010/11.

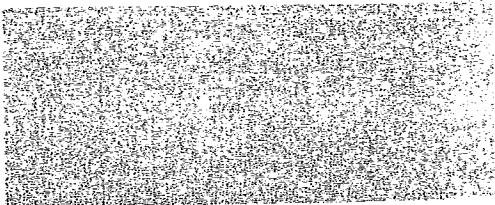
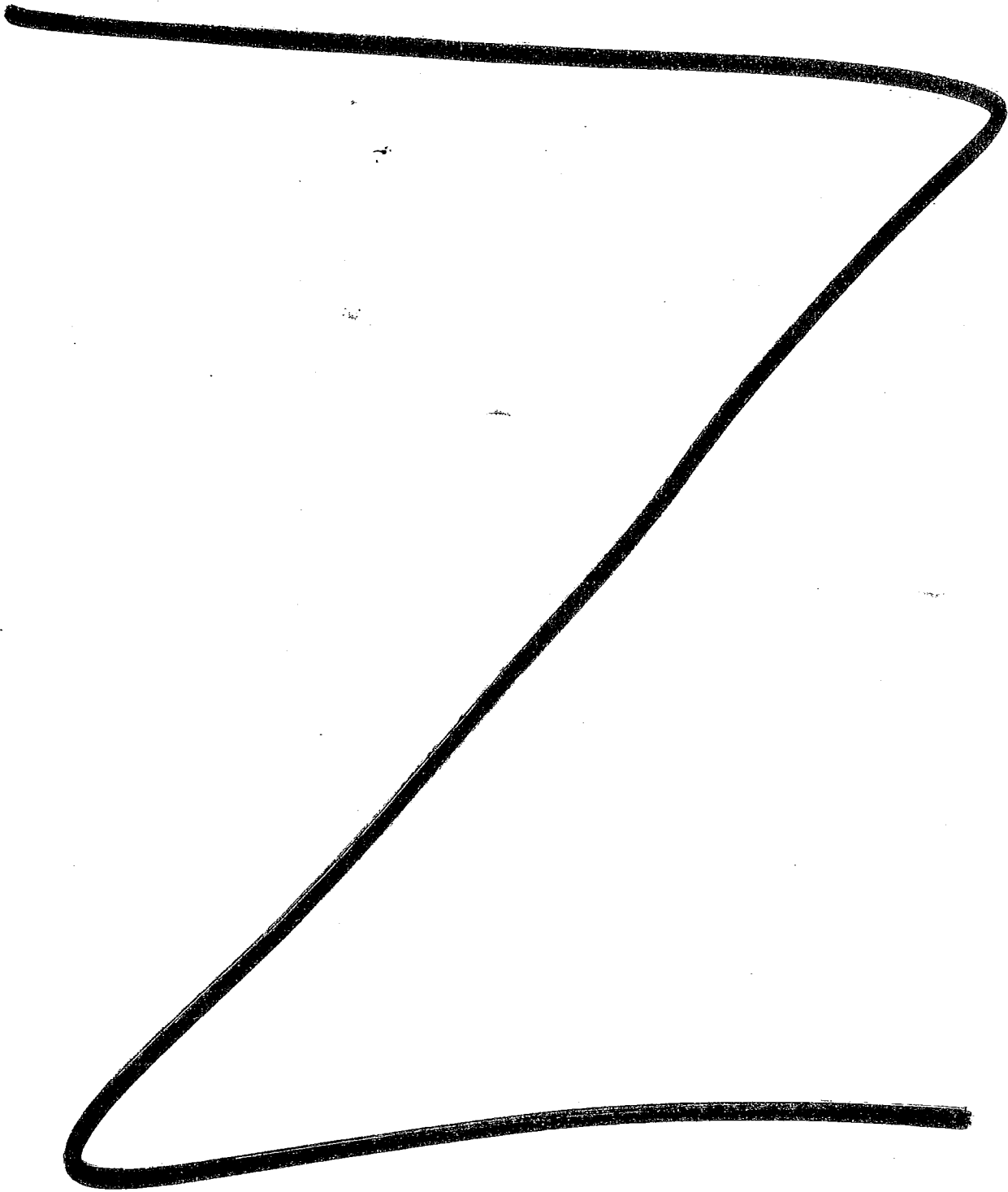
### **Theft & Loss**

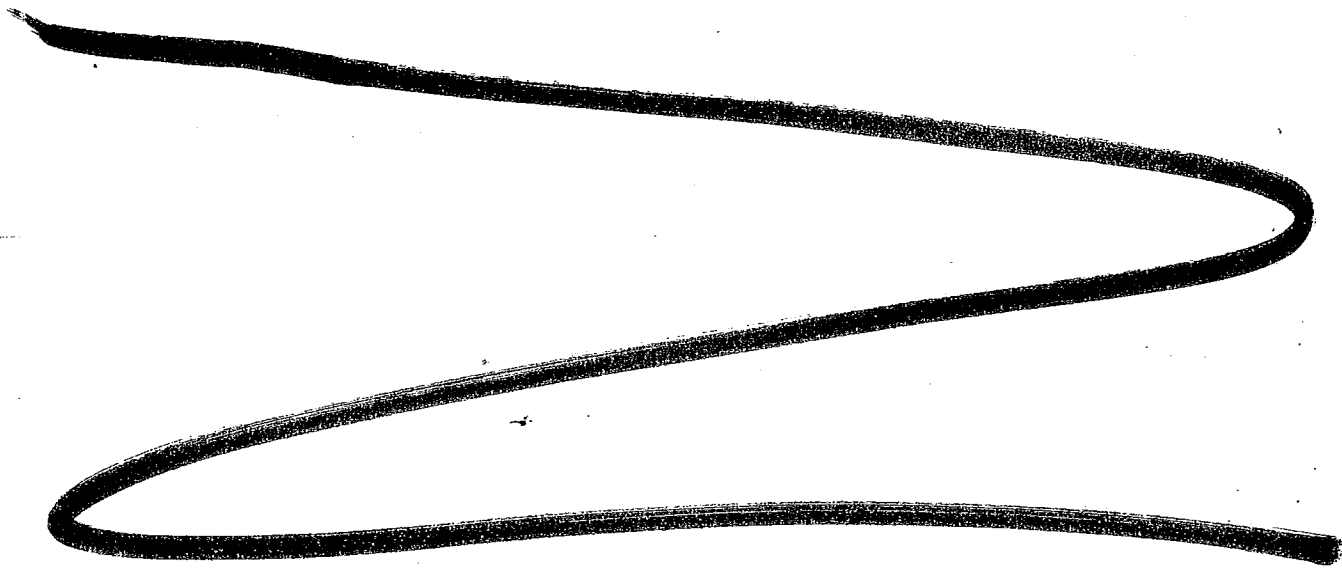
### **Security Incidents**

There were no major security incidents during the first quarter of 2010. There was one incident where a desktop computer appeared to have peer to peer networking software installed. The desktop was attempting to communicate out to the Internet and was detected by the government's 24x7 monitoring service. The investigation by the IPC and [redacted] revealed a compromised computer that was re imaged by [redacted].

Application Server Vulnerability Statistics







f

f