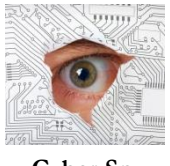
Cyber Security Environment

Government of Alberta

Who are the Threat Actors	What is the Threat?	Is the Threat To GoA Real?
 **Internal Staff**	Lack of cyber threat awareness often results in accidental loss of data confidentiality, integrity or availability when users either reveal secure information or personal credentials. **GOAL: None (accidental)**	188 cyber security incidents due to user errors in 2015 16% GoA users "clicked" on 2015 Email Phishing test 24% GoA users took online security training in 2015
 **Natural Disaster**	Natural disasters are random events that cannot be predicted impacting IT services availability (eg: events such as power outages or critical events such as tornadoes or floods.) **GOAL: None (random)**	212 Critical apps 180 Vital apps (too high!) 72% of Critical and Vital have DRPs (too low!) 50% of Critical and Vital DRPs recently tested (too low!)
 **Hacktivist**	Hacktivists look for confidential information to reveal to the outside world or perform website defacing. **GOAL: To shame the organization**	2.6B denied FW connections from 147K unique IPs in 2015 Top country of origin - denied connections: China (15%) Gov. of BC website was defaced by *"Anonymous"* in 2014
 **Cyber Criminal**	Criminals have found a safe medium to commit crimes anonymously, and make money. Crimes include fraud, identity theft, ransomware, and many other activities. Sometimes internal. **GOAL: To make a profit**	Nov to Jan: 23 PC ransomware, cost impact: $150K 90% of GoA emails (>500M) blocked annually Nov to Jan: 694 ransomware blocked
 **Cyber Spy**	Trade secrets and other confidential information that could give an edge to a competitor or provide political advantages is the ultimate goal of cyber spies. **GOAL: To gain competitive edge**	World Govs travel to China using separate throw-away devices Denied external connections also attributed to this "Hacker Hunting": SQL Injection attempts (2 China IP)
 **Cyber Terrorist**	Terrorists cyber attacks aim at taking control of systems causing service interruptions or disruptions, resulting in serious threats to human lives. Blackmail is another related threat. **GOAL: To scare or hurt people**	US Homeland reports ransomware used for funding Denied external connections also attributed to this Threat of hacking SCADA systems too serious to ignore

What Strategies Mitigate the Threats?	Mitigation Activities Or Initiatives
1) Hardening of the GoA's Cyber Security Posture	**Operation Activities** - MSS Transition - Improved Monitoring - IMT Incident Response Plan - GoA InfoSec Framework **Initiatives/Projects** - Cyber Security Toolset - CISO Service Catalog - Facilitation of InfoSec Framework Compliance - IT DRP Improvements - IT Security Risk Management Improvements
2) Increasing Information Stakeholders Awareness	**Operation Activities** - Cyber Security Part of Performance Contract - E-Learning required yearly - Email Phishing Tests **Initiatives/Projects** - New In-Class Cyber Security Training for GoA staff - Upgrade of E-Learning and other online material - New In-Class MISO training
3) Shifting Security Posture from Reactive to Proactive	**Operation Activities** - Cyber Security Ops report - Cyber Intelligence report - Tighter interactions with NCSIP, CCIRC and ASSIST - Security Clearance Level 2 **Initiatives/Projects** - Develop Cloud Access Security Framework - New Cyber Threat Intelligence Services - Update and formalize Info Sec Risk Management

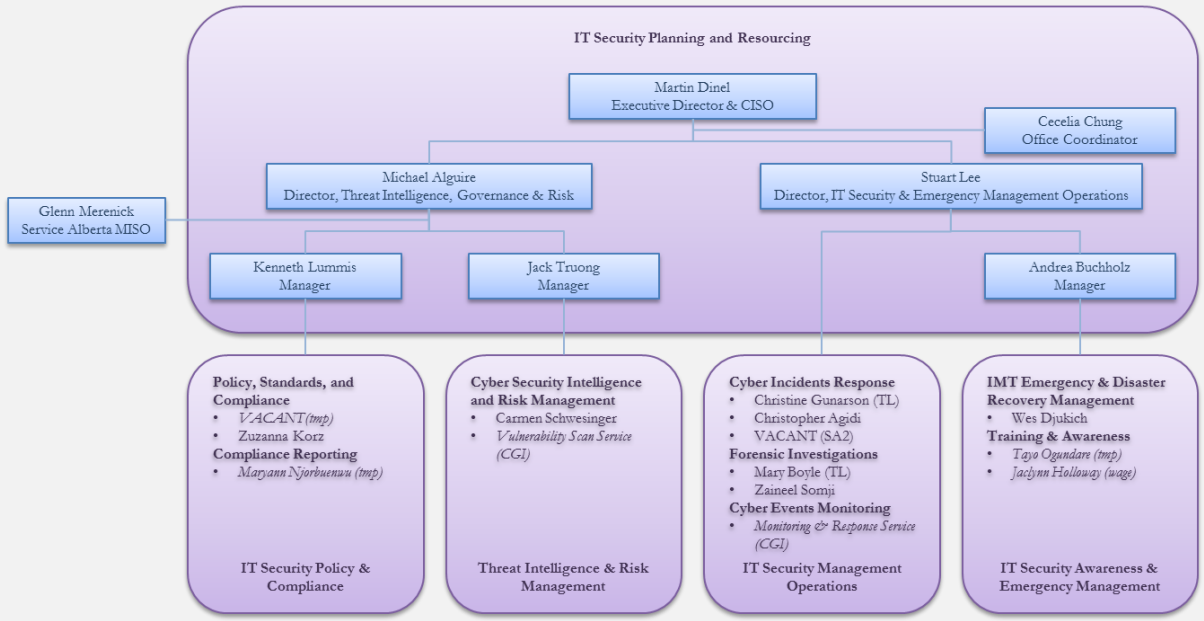
Corporate Information Security Office (CISO)

Government of Alberta

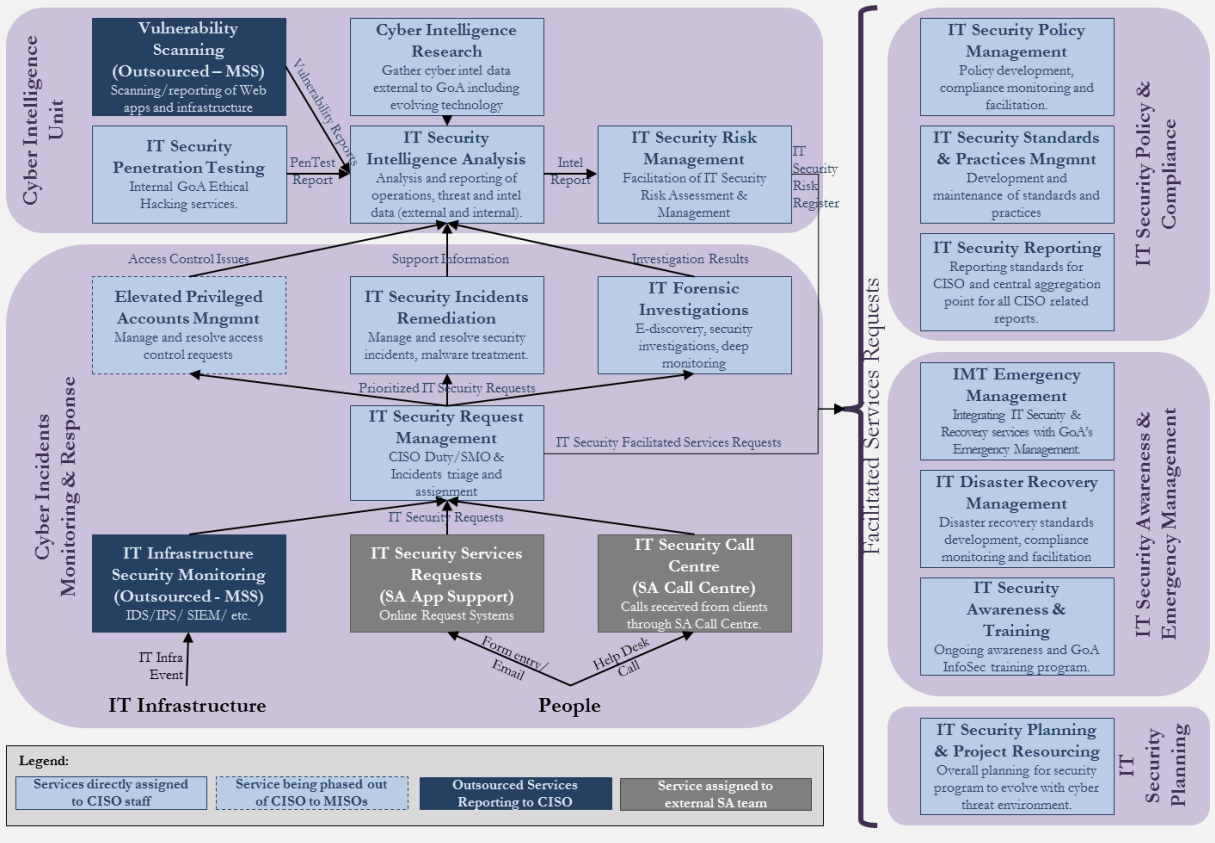
Cyber Security Incident?
Contact: DutySMO@gov.ab.ca

Cyber Security Program Question?
Contact: ciso@gov.ab.ca

CISO Team Organization



CISO Services and Teams



CISO Program Plan