RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CSV-R02

Enterprise Acquisition of Cloud Computing Services

Black Box, SaaS, Across Jurisdictional Boundaries…

Robert Hawk

Principal Consultant
RBH Enterprises
www.LinkedIn.com/in/IronManRBH

Steve Vandenberg

Senior Managing Consultant
IBM Canada
www.LinkedIn.com/in/SteveVandenberg

Disclaimer

This presentation reflects the experience and observations of the presenters with Advanced Metering Infrastructure technology on multiple programs. It does not represent information or positions specific to any project, utility, its vendors or partners.

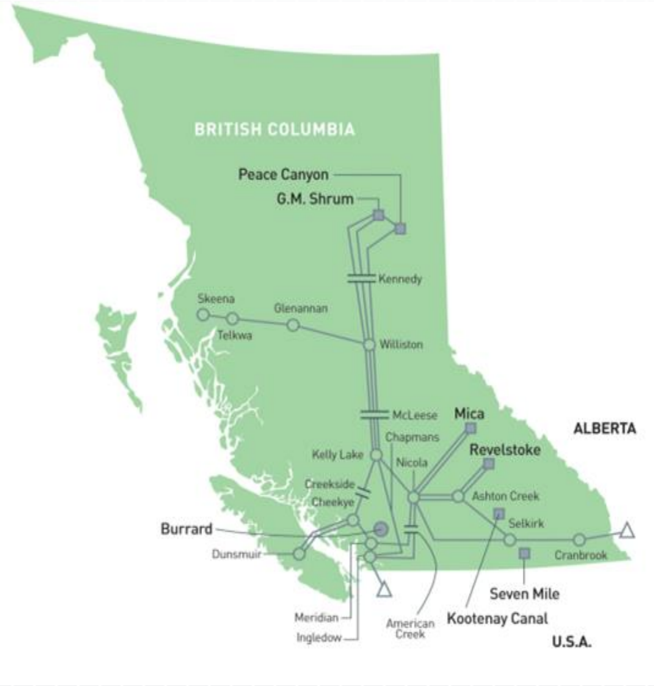
It is not a representation of the BC Hydro SMI program.

The Cloud has opportunities that must be seized

Your tools and methods don’t work here

There can be a downside

BC Hydro's AMI Deployment



- British Columbia larger than CA, OR and WA combined
- 1.9 million Smart Meters, 1000's of Field Area Routers (FAR), IPv6 network
- Deployment: 2011 through 2014
- Cost: $$$
- Energy Theft Analytics a key part of business case

Energy Theft Analytics

- Energy theft in BC was a large problem estimated at >500 GWh/yr
  - Primarily due to marijuana grow ops
- Improved energy diversion detection business case:
  - Was estimated to be

    45% of the total SMI project benefits
  - Electrical safety improvements
- Cloud based system was chosen
- Contract was awarded to a US company

Across Jurisdictional Boundaries

- Canadian privacy laws control transmission of Personally Identifiable Information (PII) over legal jurisdictional boundaries including to the US
  - Freedom Of Information and Protection Of Privacy Act (FOIPPA) forbids transfer of data outside of Canada
  - Cloud provider can establish Canadian data center in compliance with FOIPPA requirements
  - Cloud provider can administer the operation from the US. Data and algorithms can run in the Canadian cloud and never in the US

Requirements

- Working at the intersection Cloud & Big Data
  - Volume – terabytes
  - Variety – 3 to 20 types
  - Velocity – multiple reads per day

- Gathering data from the Smart Meter fleet millions and sending to the provider for analysis
- Producing actionable power theft lead reporting for the investigators

Solution

- Cloud provider provides theft analytics with Software as a Service (SaaS) Black Box
- Uses proprietary and patented processes including algorithms that the cloud provider will not release to client
- Black box providers usually don’t allow security assessment or testing within their security perimeter
- Public/Private cloud and Identity Federation to the cloud provider is not necessary for architecture requirements because the relationship is based on data transfer and report production

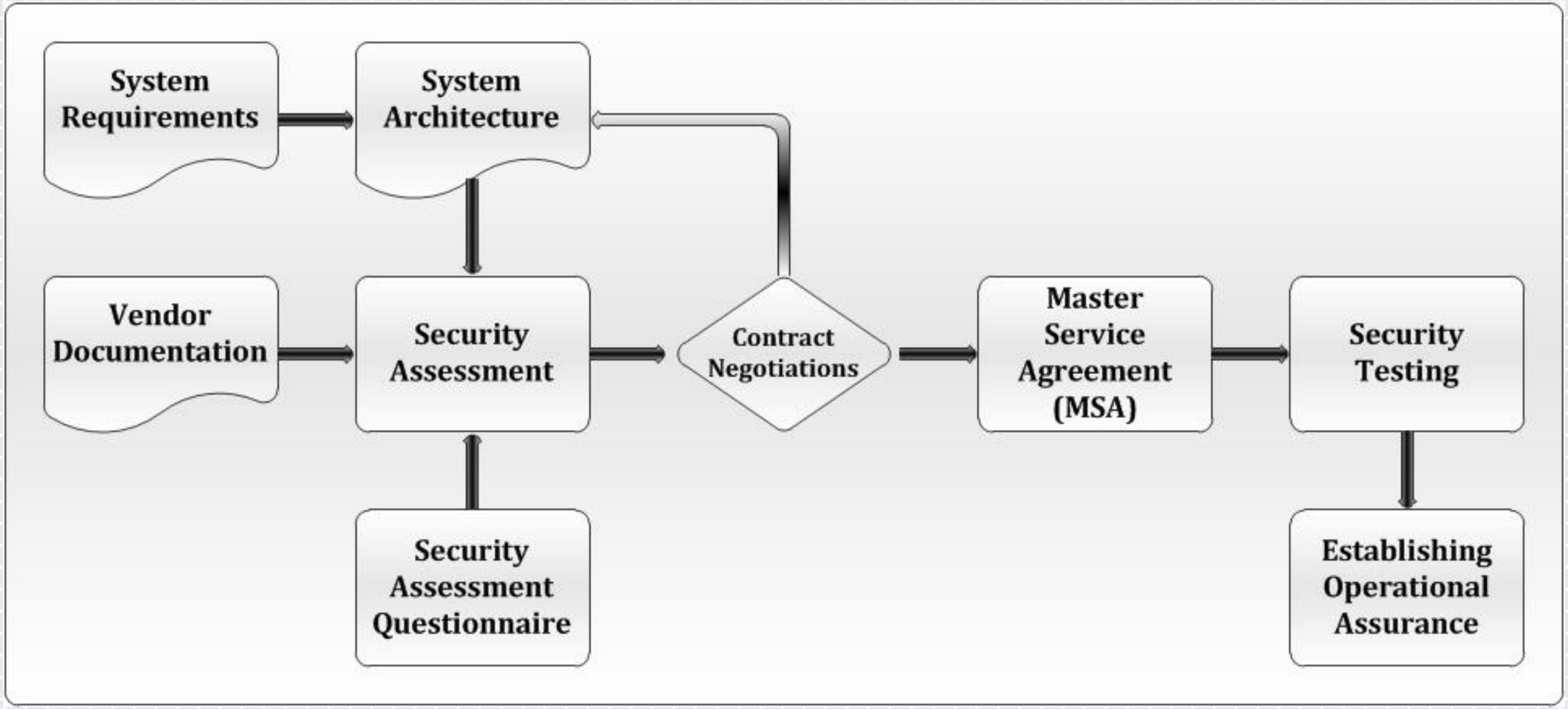
Standards Based Security

- Security Team findings drive product and process changes
- Common set of principles that client and the cloud provider can accept is needed
- Architecture, Security Assessment and Testing should be based on standards and frameworks provided by:
    - Cloud Security Alliance e.g. Security Guidance v3.0
    - National Institute of Standards and Technology (NIST) Special Publications (SP) e.g. SP800-144, SP800-146

Let Risk be the Guide

- Use case created for each test case
  - Security assessments used to determine risk rating
  - Use risk rating to prioritize security resources and efforts
- Risk assessment focus
  - Access Control
  - Encryption
  - Interfaces and communication channels

Security Process



Security Vetting

- Security Architecture
  - Cloud Security Alliance and NIST considerations for best practices implemented in the architecture
  - Focus on connections to the cloud provider and treatment of PII inside the cloud
  - Focus on data transfer and storage architecture both for initial upload and ongoing communications
- Security Assessment
  - Creates and confirms alignment of policies between client and the cloud provider

Security Assessment

- The Security Assessment investigates Administrative and Technical Controls for:
  - Data Communications
  - Data Transfer
  - Based on client’s policies e.g.
    - ISO 27000 Series, NIST IR 7628, Cloud Security Alliance

Security Testing

- Tests and verifies security implementation is in alignment with the architecture
- Tests for proper use of username, passwords, and key generation in alignment with client's corporate policy
- Tests transfer mechanisms such as SSH for compliance to best practices
- Security tools – e.g. Codenomicon, Nessus and AppScan can be used to check infrastructure and application on the client side
- *If security testing of cloud service provider's infrastructure is done, must have agreements in place with liabilities determined and accepted*

Master Service Agreement

- Data at rest and in transit to have strong encryption
- Access control based on principle of least privilege with role based requirements
- For Situational Awareness monitoring, logging and reporting by the cloud provider is required
- Configuration Management & Change Control is required
- Data destruction to best practices is required
- Security Awareness training for cloud provider’s staff is required

Master Service Agreement

- Physical segmentation from other clients’ processing and data storage required
- Data transfer across jurisdictional boundaries must comply with applicable rules e.g. BC FOIPPA
- Innovative business and process solutions are required to monitor and maintain servers but restrict data flow
- Client’s right to audit agreed aspects of the cloud provider’s security is required

Benefits

- Security becomes a business enabler
  - Security paranoia is replaced with security innovation
  - Legal, business and privacy stakeholder needs are met
  - Best business and technology solution is implemented securely
- Master Service Agreement incorporates security
- Auditable processes are implemented for cloud security
- Relationship between client and cloud provider is set up for long term success

Apply this when Acquiring a Cloud Service

- Define security, privacy and compliance requirements
  - Make them a part of the architecture and the contract
- Identify requirements imposed by jurisdictional boundaries
  - Engage privacy, legal and business teams to inform compliance options
- Focus on connections to the cloud provider and treatment of protected information
- Use Security Assessment to confirm alignment of policies and standards between client and the cloud provider

Apply this when Acquiring a Cloud Service

- Address the Security Assessment findings and client's right to audit in Master Service Agreement
- Test to verify security implementation is in alignment with the approved architecture – e.g. Nessus, Code Review, Test Passwords, SSH Encryption Keys, etc.
- If security testing of cloud service provider's site or infrastructure is to be done, must have agreements in place with liabilities determined and accepted
- The contract with the cloud provider becomes the principal security lever, not the client's security infrastructure

References

- BC Hydro SMI Business Case

  https://www.bchydro.com/content/dam/BCHydro/customer-portal/documents/projects/smart-metering/smi-program-business-case.pdf

References

- Cloud Security Alliance: SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

  https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

- NIST SP800-144 “Guidelines on Security and Privacy in Public Cloud Computing”

  http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

- NIST SP800-146 “Cloud Computing Synopsis and Recommendations”

  http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

Questions?

Robert Hawk

Principal Consultant
RBH Enterprises
www.LinkedIn.com/in/IronManRBH

Steve Vandenberg

Senior Managing Consultant
IBM Canada
www.LinkedIn.com/in/SteveVandenberg