SPARTAN CONTROLS

Experience Industrial Innovation

Cloud based security - Protection of utility dispensing services

Joanne Moore

November 7th, 2022

CANADA'S BEST MANAGED COMPANIES
Platinum member

Cybersecurity Threats

Great Australian Hack Sends Wakeup Call to Complacent Companies

Hackers hit cybersecurity conference

Noel Towell and Kishor Napier-Raman
October 24, 2022 — 7.30pm

Save | Share | A A A

The Australian Institute of Company Directors (AIDC) had some solid names lending support to the launch of the institute's new set of "cybersecurity governance principles" – a very hot topic in the wake of the Optus and Medibank Private hacks – including the federal minister in charge **Clare O'Neil** and Cyber Security Cooperative Research Centre CEO **Rachael Falk**.

Newfoundland and Labrador healthcare compromise

The Newfoundland and Labrador healthcare system was paralyzed on October 30, 2021, when cybercriminals compromised its networks. Healthcare providers could not access internal communications or diagnostic information, forcing them to adopt a paper-based approach to appointments and emergency procedures. Thousands of medical procedures and appointments were delayed. In addition to service disruptions, sensitive information pertaining to thousands of staff and patients was stolen. [52]

Personal Story

1. Password compromised on a website (Pinterest)
2. Same password was used for alternate accounts (including PayPal)
   PayPal uses 2 factor authentication
3. Similar username / same password used for cellular phone online account.
   Gains access to personal details
4. Hacker uses information gathered to assign my phone number to their device
5. Now have access to transferring funds in my PayPal account

Attackers just have to be lucky once, but defenders have to look at all the potential risks all the time

Cybersecurity - Basics

- **Cybersecurity:** The *practice of protecting critical systems and sensitive information from digital attacks*.

- Protecting your critical infrastructure as a company is not a one-time endeavour, need to be constantly monitoring for potential cyber-attacks

Cybersecurity Statistics

- Fraud and scams, including malicious cyber threat activity such as phishing, result in significant financial losses.

The impact of fraud so far this year

As of September 30, 2022

Reports of fraud:
68,259
(107,139 in 2021)

Victims of fraud:
43,476
(68,061 in 2021)

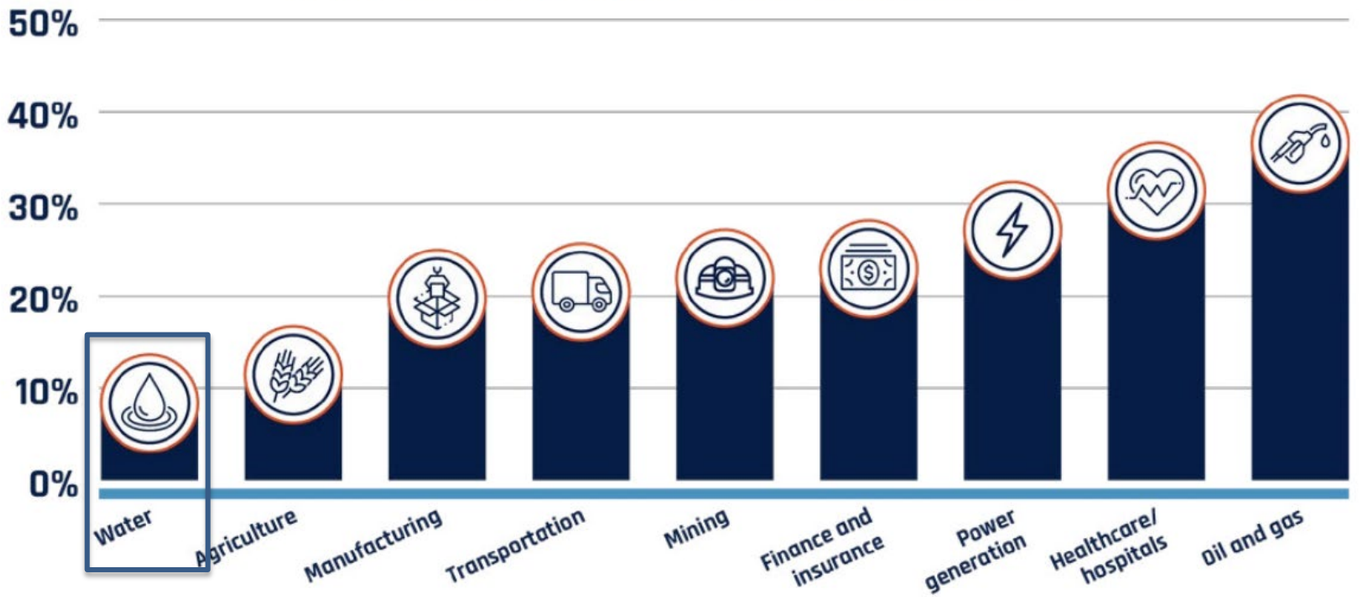
Lost to fraud:
$362.7 M
($383 M in 2021)

https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

CANADIAN CENTRE FOR CYBER SECURITY

National **Cyber Threat** Assessment

Figure 7: Percentage of CI sectors reporting a cyber incident (2019)[60]



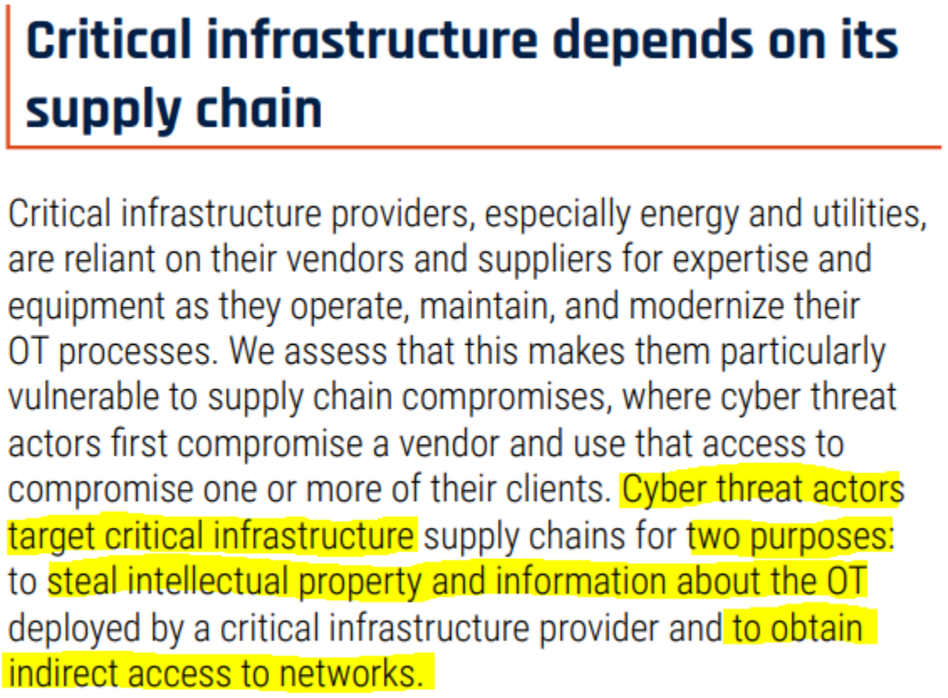
https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

Cybersecurity Statistics

- What breaches to critical infrastructure can cause:
  - Service disruptions
  - Breaches of personal / sensitive / valuable data

NEWFOUNDLAND AND LABRADOR HEALTHCARE COMPROMISE

The Newfoundland and Labrador healthcare system was paralyzed on October 30, 2021, when cybercriminals compromised its networks. Healthcare providers could not access internal communications or diagnostic information, forcing them to adopt a paper-based approach to appointments and emergency procedures. Thousands of medical procedures and appointments were delayed. In addition to service disruptions, sensitive information pertaining to thousands of staff and patients was stolen.[67]



Critical infrastructure depends on its supply chain

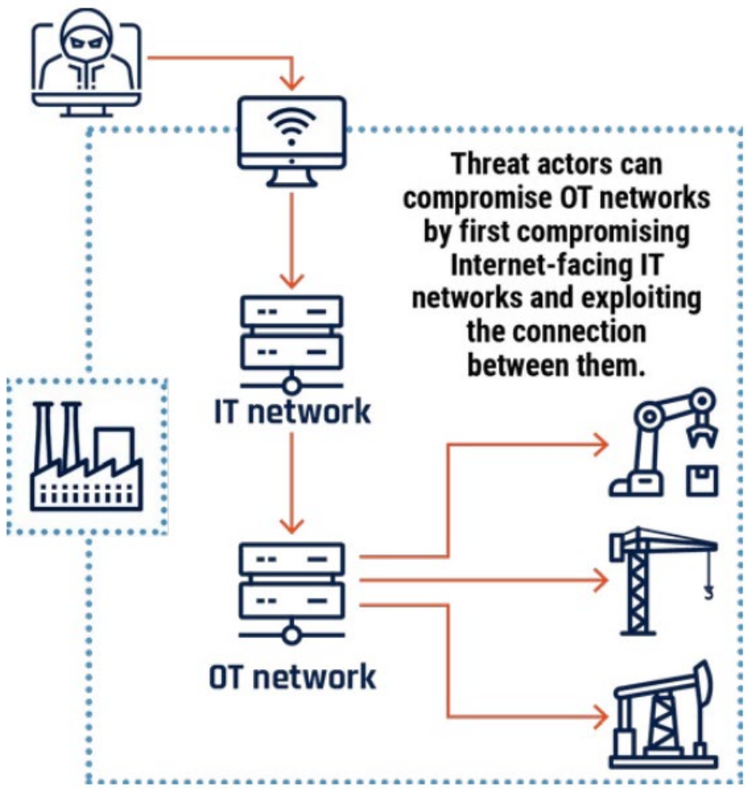
Critical infrastructure providers, especially energy and utilities, are reliant on their vendors and suppliers for expertise and equipment as they operate, maintain, and modernize their OT processes. We assess that this makes them particularly vulnerable to supply chain compromises, where cyber threat actors first compromise a vendor and use that access to compromise one or more of their clients. Cyber threat actors target critical infrastructure supply chains for two purposes: to steal intellectual property and information about the OT deployed by a critical infrastructure provider and to obtain indirect access to networks.

https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

Cybersecurity – Water Utilities

Connected OT increases critical infrastructure's cyber threat surface

Figure 6: OT compromise through IT networks

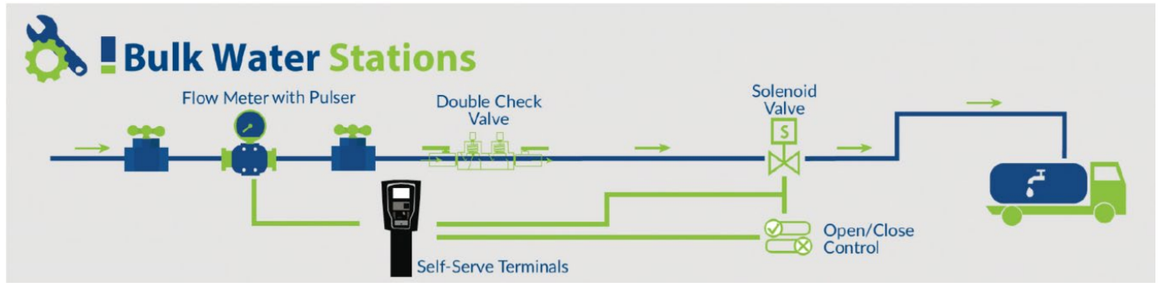


- Best to isolate operational network from the internet, but this is certainly not always possible
  - Need to access data not available locally for operation
- Companies can have specific requirements or a network architecture that describes network communications the company wishes to follow

https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

Industry Example – Computrol Bulk Water Fill System

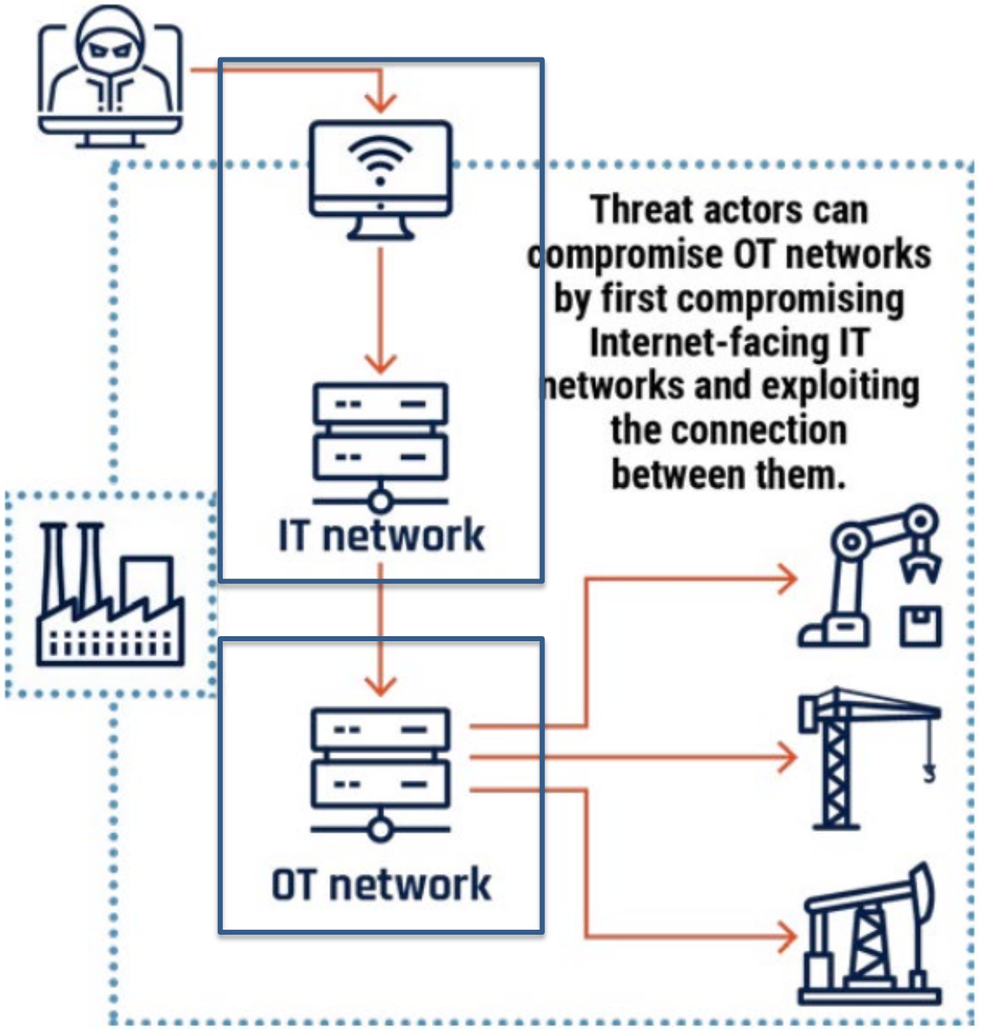
- Bulk water loading station:
  - Water loaded through a hose, typically onto a truck
  - Need to track how much water is used/sold
  - Includes Measurement system as well as a kiosk for producing a receipt



Industry Example – Computrol Bulk Water Fill System

- At the terminal or “kiosk” need to track:
  - amount of water loaded
  - who received the water
- Need for data external to the system
  - Administrator/Operations wants to track total volumes
  - Need control over who can take water
  - Want to bill customers using the data from the kiosk
  - Want to be able to manage any restrictions
  - Need an IT network connection – *Need to be aware of cyber threats*

Figure 6: OT compromise through IT networks



Project Example– Cyberthreat identified – System upgrade needed

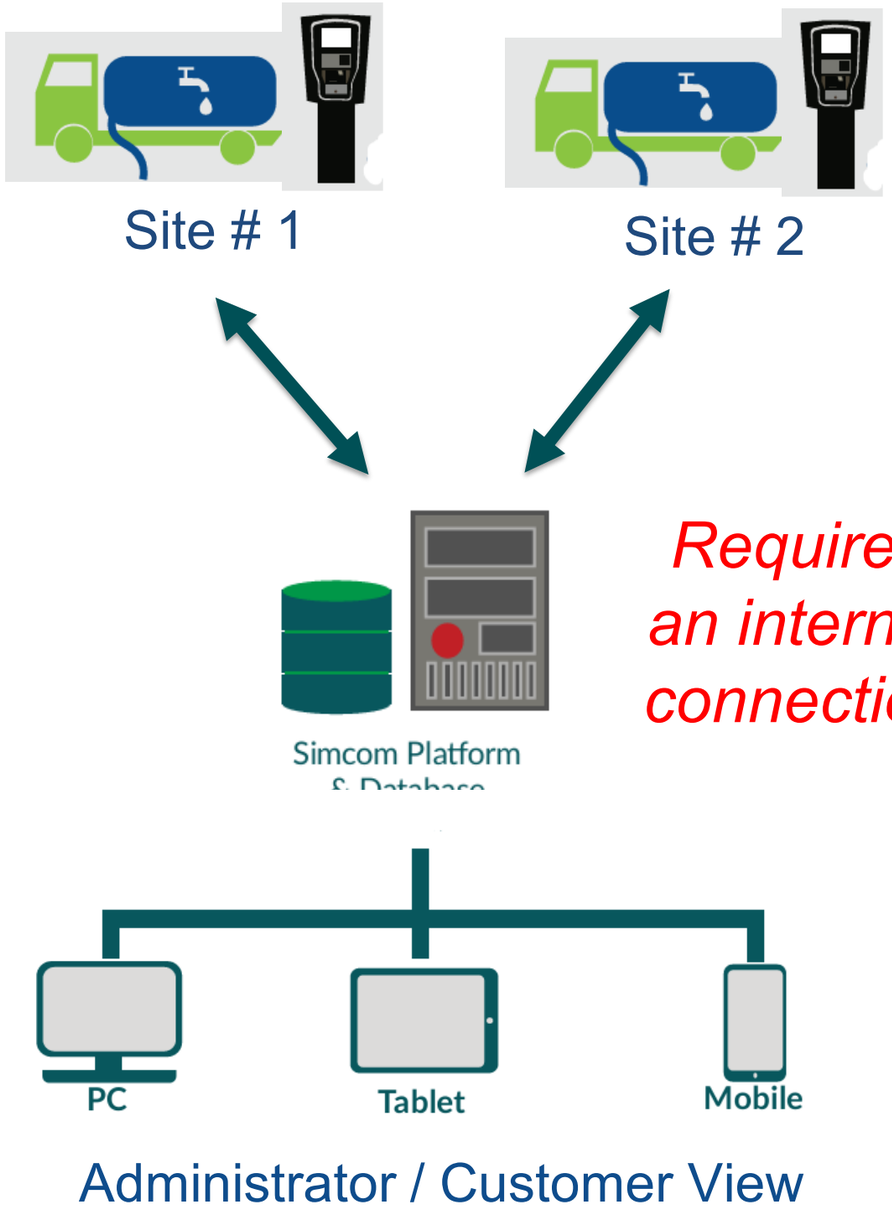
- Approached for a system upgrade some older style bulk fill stations for a city in Western Canada
  - The kiosk was connected to the web for moving data back/forth into the system
- One of the paramount requirements on the request was to have a cloud-based software solution.

  “The city would require the system to be separate from their network, and all the upgrades to be management by the Proponent”
- After proposal completed, we heard this feedback:

  “When we had a cyberattack on the city, we determined the gateway was through water sales… This is how they eventually got into our system… We want to remove this risk and provide much greater security as a whole.”

Project Example– Usage Requirements

- *Cloud Based Requirement:*
  - Main software server needs to reside in the cloud
  - Updates occurring automatically without intervention of city
  - Data integration of multiple sites
- *Functional Remote Requirements:*
  - View of volumes purchased, customer account balances
  - Ability to change rates, inactivate accounts



Cyber Security – Layers to Prevent Crime

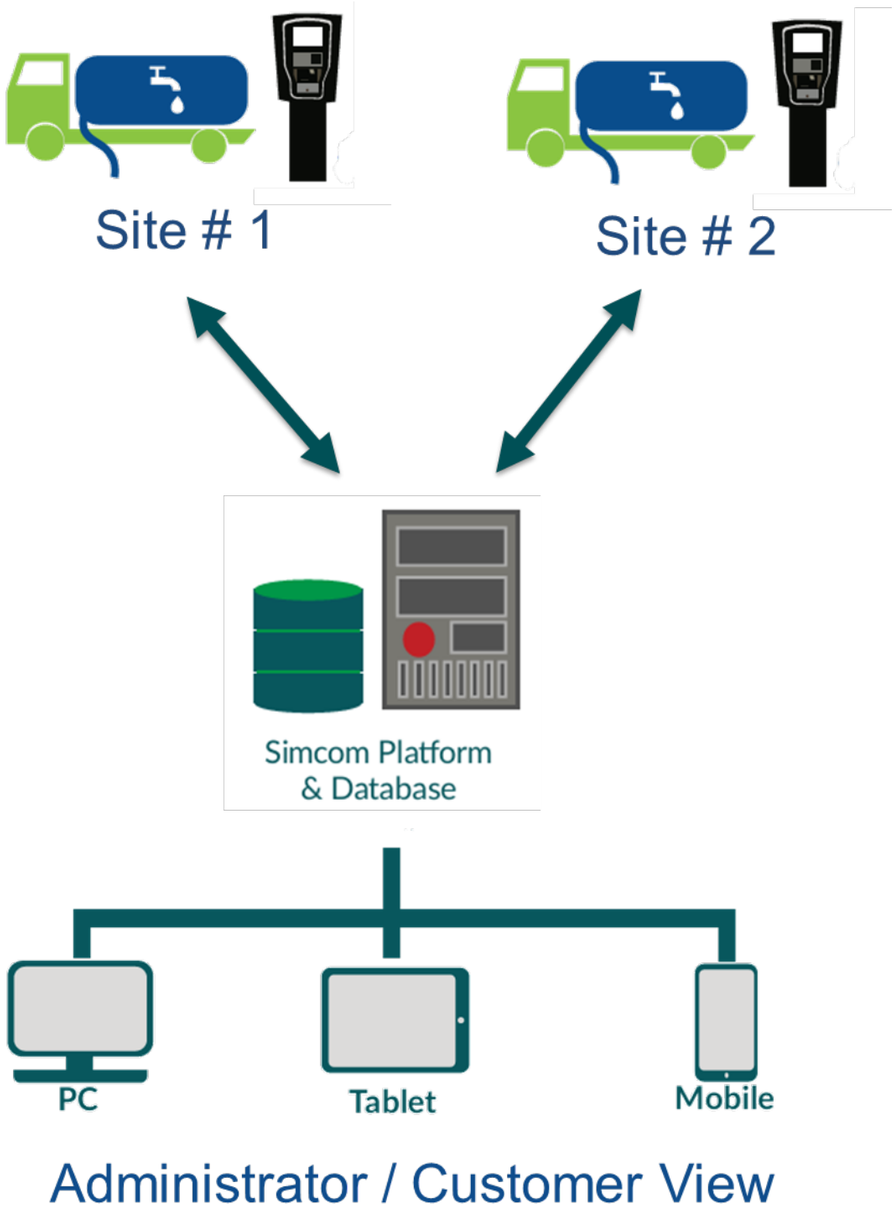
How do we protect the data?

Network Security – measures for protecting a computer network from intruders (Access control, Antivirus, etc.)

Application Security – Processes that help protect applications operating on-premises and in the cloud. Security should be built into applications at the design stage, with considerations for how data is handled, user authentication, etc.

Cloud Security – Involves encrypting cloud data at rest (in storage) and in motion (as it moves between locations) and in use (during processing) to support requirements

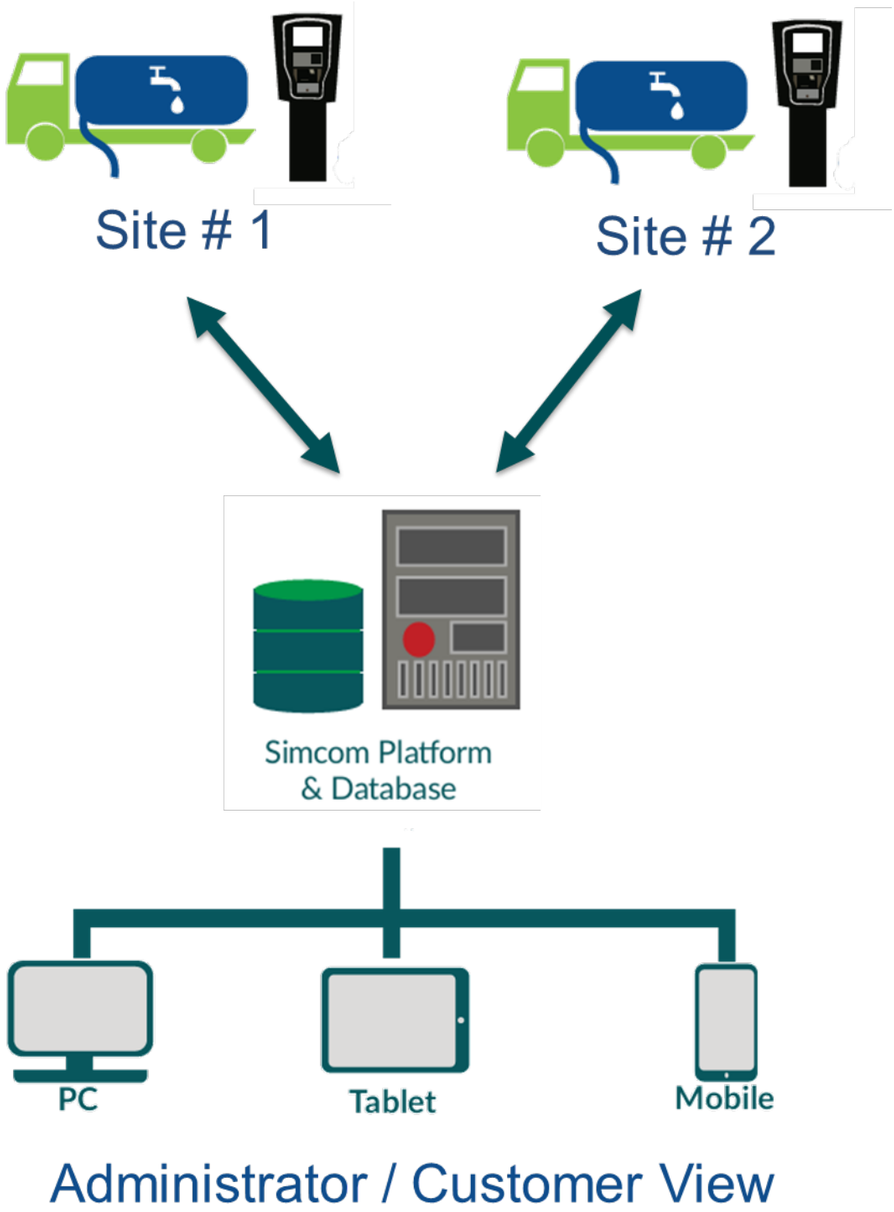
… and others methods (ie. training, disaster recovery, etc.)



Cyber Security – Layers to Prevent Crime

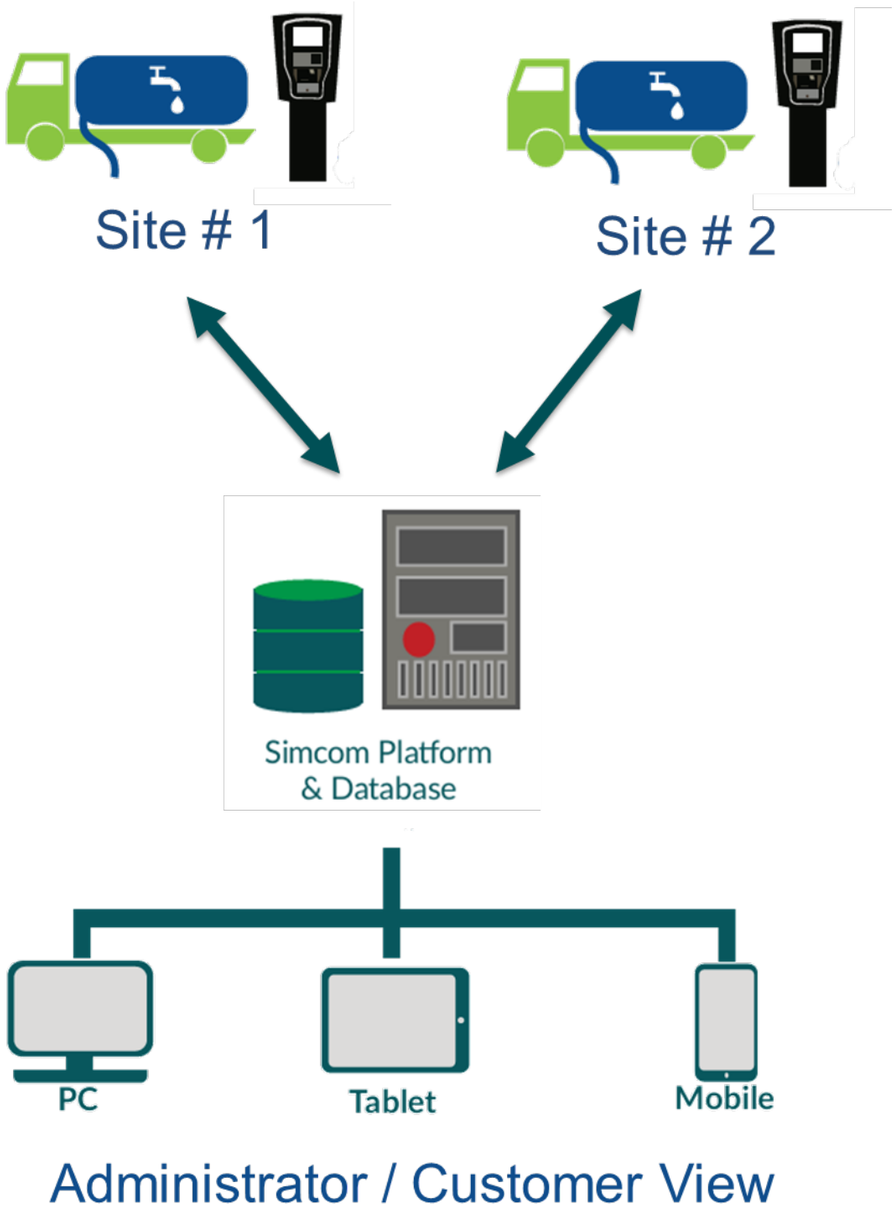
- Use case: Office administrator needs to software to make a change to a system user on the kiosk.

How is the data protected?



Cyber Security – Layers to Prevent Crime

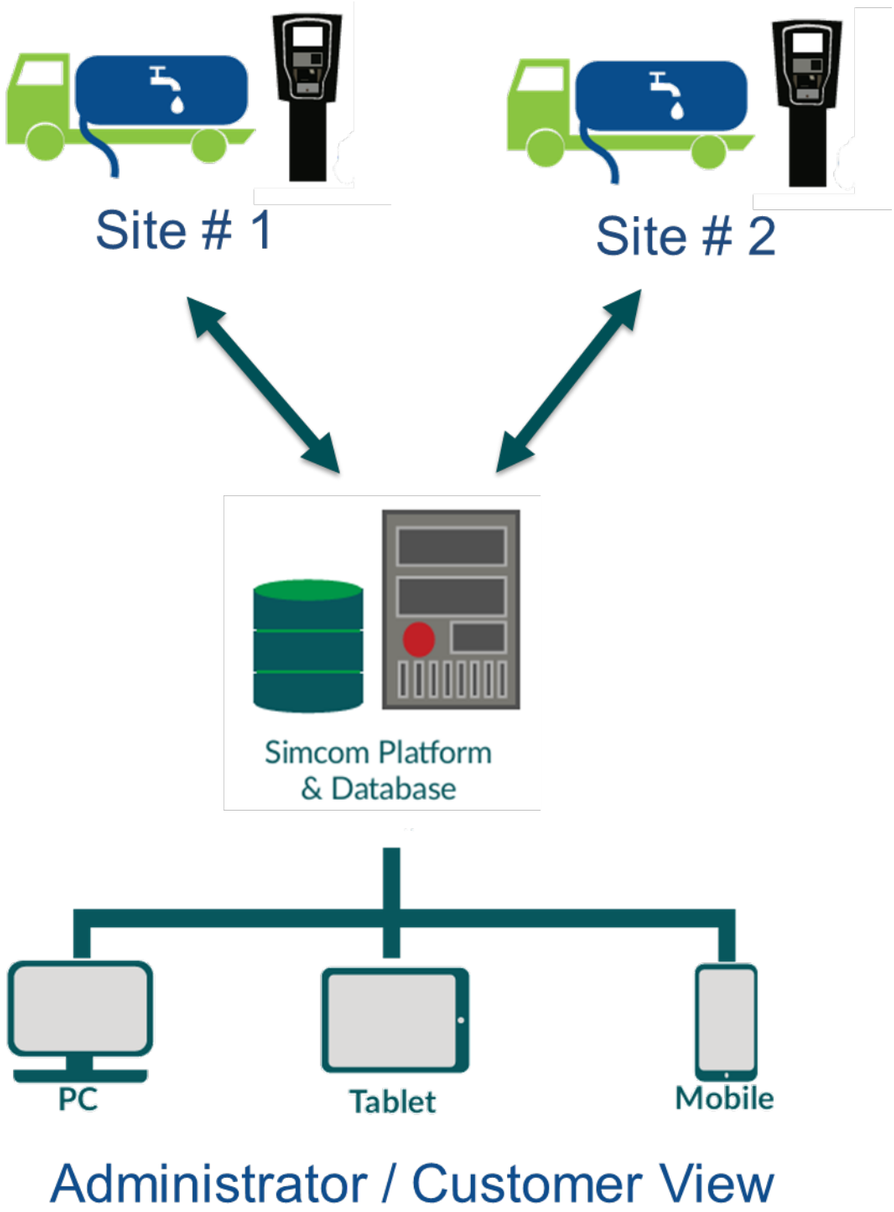
- **Network Security:**
  - For the Web-based application have login credentials for security purposes
  - Option to have 2 factor authentication to make it even more secure
  - Multiple levels of permissions specific to the user, ie. a customer using the system would have minimal information compared to a site administrator



Network Security – measures for protecting a computer network from intruders (Access control, Antivirus, etc.)

Cyber Security – Layers to Prevent Crime

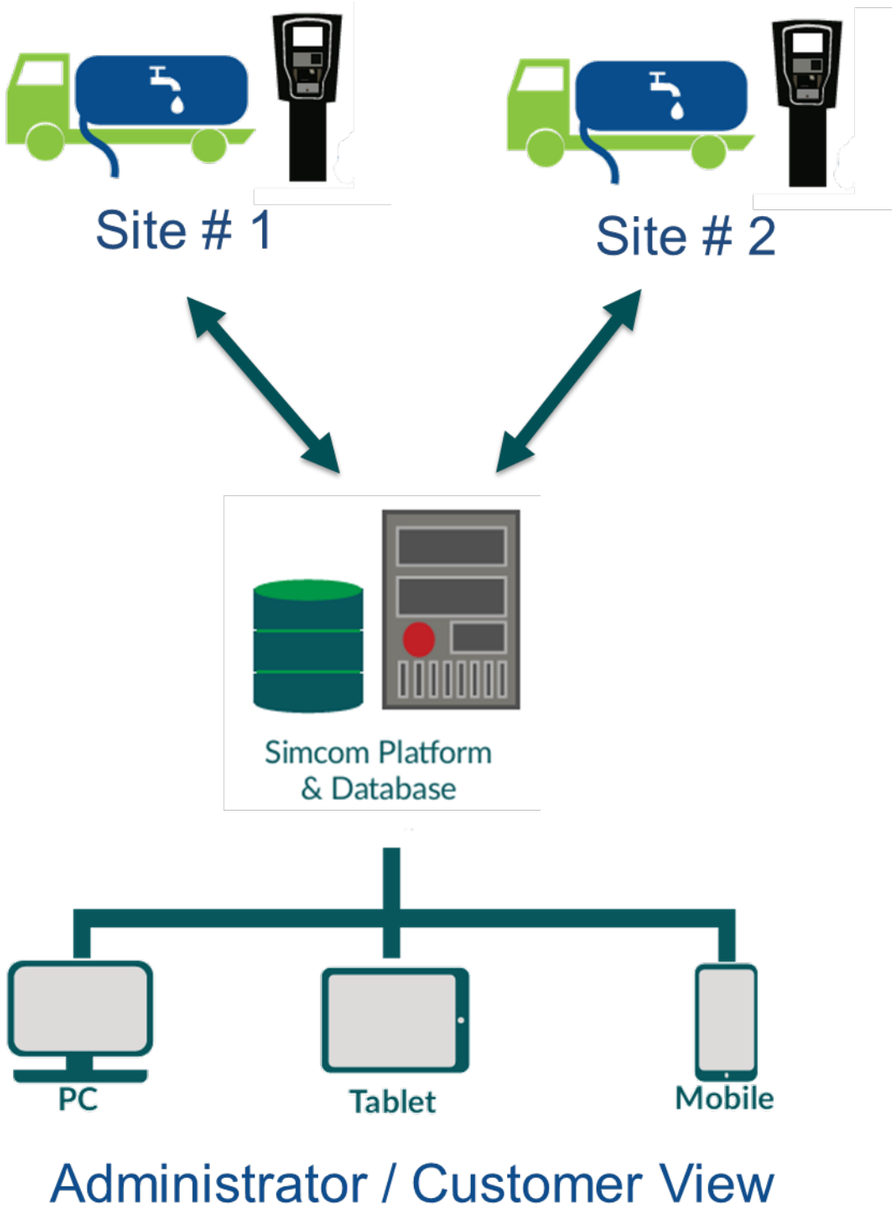
- **Application Security:**
  - Server is located in the cloud.
  - Communication from user application to the database is protected:
    - End to end encryption
    - Web-based application uses a secure website (https://)



Application Security – Processes that help protect applications operating on-premises and in the cloud.

Cyber Security – Layers to Prevent Crime

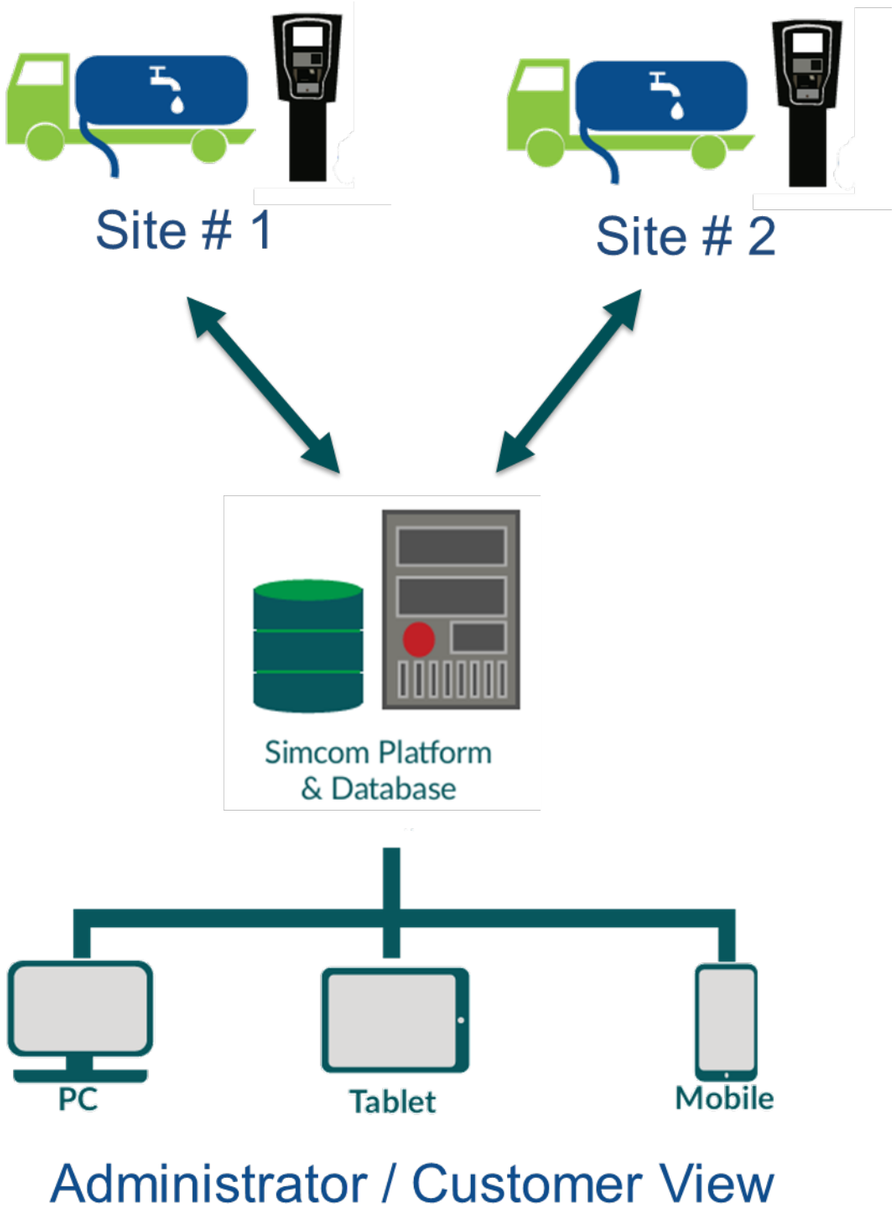
- **Cloud Security**
  - Encryption of database (TLS 1.2 Encryption protocol). If it was hacked, the data would be encrypted
  - Limit traffic to known IP addresses. (ie. each Terminal has a known IP address, cannot write to the database if an external IP used.



Cloud Security – Involves encrypting cloud data at rest (in storage) and in motion (as it moves between locations) and in use (during processing) to support requirements

Cyber Security – Layers to Prevent Crime

- **Cloud Security**
  - Hosting Environment – utilizes one of the largest Canadian data centers. Multilayer security offered to protect against attacks
    - SSAE 16 SOT 1 Compliant

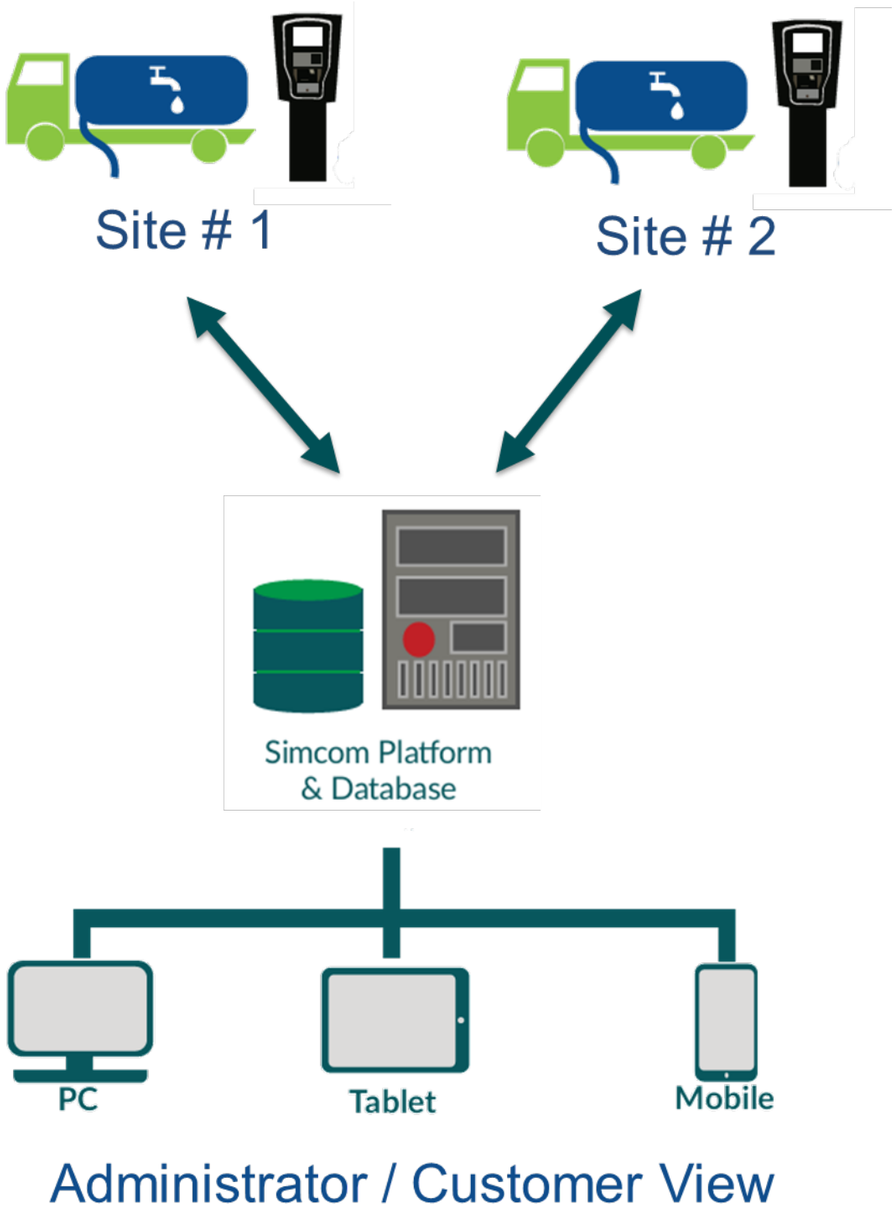


Cloud Security – Involves encrypting cloud data at rest (in storage) and in motion (as it moves between locations) and in use (during processing) to support requirements

Summary

- Need to ensure if your operational system is connected to the web to follow proactive measures to ensure your corporate network stays protected

- Protecting your critical infrastructure as a company is not a one-time endeavor, need to be constantly monitoring for potential cyber-attacks



Contact Me

Joanne Moore

Phone

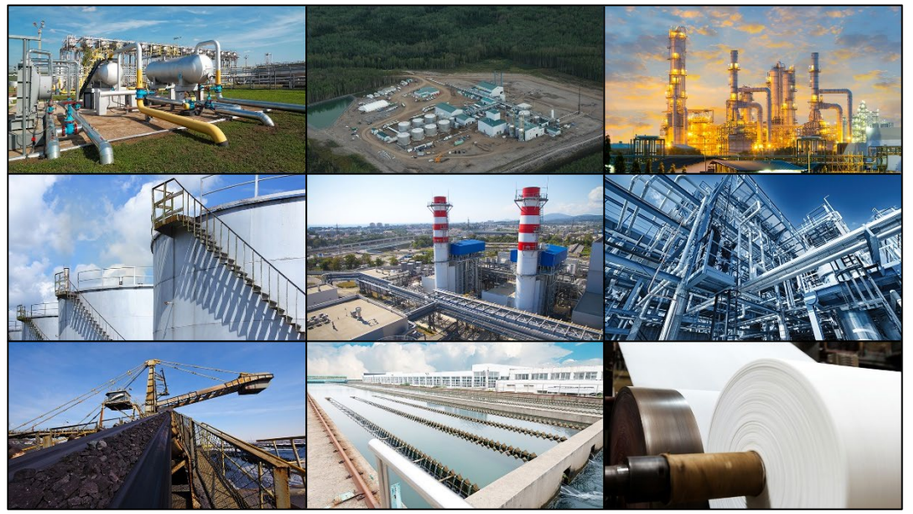
(403) 695- 2607

Email

Moore.joanne@spartancontrols.com

24/7 Support

+1 (877) 278-6404



join the conversation