



TELUS

Defensible and Beyond

Mike Vamvakaris
Director and Head of
Cyber Security Consulting

November 2017

 **TELUS** | Business

Digital transformation brings many benefits...

Communication and
Collaboration



Autonomous and Artificial
Intelligence (AI)



Internet of Things (IoT)



...it also brings new risks



YoY growth in cybersecurity incidents in Canada



Organizations reported being victim of a phishing attack



Businesses fell victims to cyber ransom attacks in 2016



Organizations have systems/controls for advanced threats



IT skills gap in Canada in 2016: key areas include IT operations, security and programming

Source: IDC, Cisco, Hootsuite, Gartner, Statista

What's at stake?

35% of organizations were **hit with ransomware** in 2017



1 out of 5 couldn't conduct business for an hour to a day or more

Attackers can typically get **admin access within 3 days**



100 days before an organization **detects a breach**

\$86k to \$5.78M



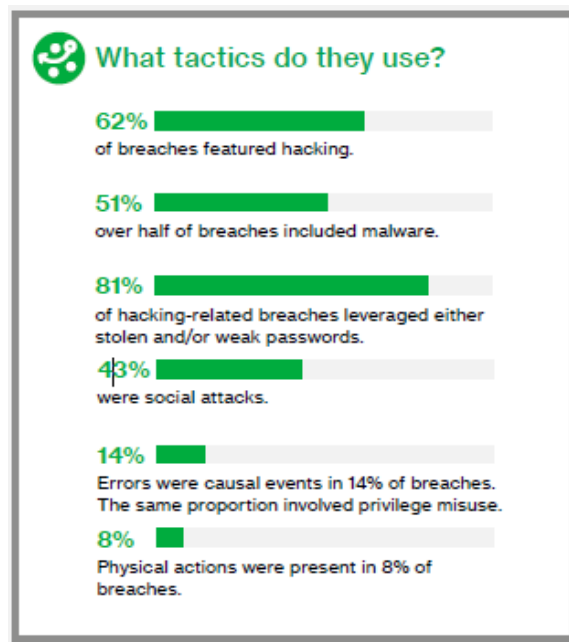
The costs of single cyber attacks are **increasing**

Source Malwarebytes 'Second Annual State of Ransomware', Ponemon Institute, Mandiant M-Trends 2017

How are they getting in? | Emerging threats

- Ransomware
- Phishing attacks
- DDoS attacks
- IoT / weak passwords
- Hardware / Firmware targets
- Mobile device attacks
- Social media fake ads
- Hacking personal devices – smartphones, tablets

Source: 2017 Verizon DBIR



Why Defensible? | No organization is immune to attack



Defensible Security – Definitions (1/3)	Defensible Security – Definitions (2/3)	Defensible Security – Definitions (3/3)
<ul style="list-style-type: none"> Access Control <ul style="list-style-type: none"> policy is documented, followed, reviewed, and updated regularly address onboarding, off-boarding, transition, and deactivation of users reviews, limit and control use of administrative privileges employees/contractors/vendors should be authorized to use conflicting duties and areas of responsibility reduce incidents of fraud and other abuse multi-factor authentication is required for networks system accounts unenable/use multi-factor (eg. password aging, length/complexity, etc.) Asset Management & Disposal <ul style="list-style-type: none"> policy is documented, followed, reviewed, and updated regularly includes both hardware and software and inventory must include name of system, location, and value assets are added to inventory on commission disposal requirements are based on the asset Backup & Retention <ul style="list-style-type: none"> policy is documented, followed, reviewed, and updated regularly regular backups are taken and tested regularly frequency and completeness should be based on business requirements (eg. 6 months for high value information) Business Continuity Plan (BCP) <ul style="list-style-type: none"> plan is documented, followed, reviewed, and updated regularly Change Management <ul style="list-style-type: none"> policy is documented, followed, reviewed, and updated regularly changes to production environments must be controlled Criminal Record Checks <ul style="list-style-type: none"> employees must complete a satisfactory criminal record check and be required to proactively disclose any criminal record 	<ul style="list-style-type: none"> Defence in Depth for Endpoints and Networks <ul style="list-style-type: none"> endpoints include servers, desktops, laptops, tablets, mobile devices networks include wired and wireless and require secure perimeter, network segmentation, and known ingress/egress points controls must exist to prevent, detect, and respond to security incidents technologies must include firewall, intrusion prevention, web content filtering, email content filtering, and anti-virus at a minimum systems must be hardened (eg. default passwords and shared accounts may not be used, unnecessary services are disabled, insecure protocols disabled) additional controls may be required to mitigate risk to your organization Disaster Recovery Plan (DRP) <ul style="list-style-type: none"> plan is documented, followed, reviewed, updated, and tested regularly Incident Management <ul style="list-style-type: none"> policy is documented, followed, reviewed, updated, and tested regularly Information Security Classification <ul style="list-style-type: none"> classification is documented, approved, communicated, and followed employees must understand not all data is created equal, some data is more sensitive than others and should benefit from greater controls employees should possess only the sensitive information they need, handle it carefully, and label it as appropriate sensitive information must be encrypted in-transit and at rest prohibit production data in test environments unless security controls are equivalent to production or better Information Security Policy <ul style="list-style-type: none"> policy is documented, approved, followed, reviewed, and updated regularly policy should be standards-based in order to evolve over time include Appropriate Use so employees know what they may and may not do Information Security Program <ul style="list-style-type: none"> program is documented, approved, executed, reviewed, and updated regularly align with organization's mission, vision, and goals provides clear direction on security strategy Logging & Monitoring <ul style="list-style-type: none"> collect system logs to determine who did what when, retain according to retention policy, correlate and monitor to identify and act on suspicious activity 	<ul style="list-style-type: none"> Physical Security & Visible Identification <ul style="list-style-type: none"> policy is documented, followed, reviewed, updated, and tested regularly facilities must benefit from adequate controls (eg. alarms, fences, locks, intrusion detection, cameras, guards) use visible identification (including picture) and do not Program and Course <ul style="list-style-type: none"> program and course for employees regularly update security course for employees announcements and impacts to business such as not sharing suspicious links and attachments, reporting security incidents, locking inactive systems, concealing valuable information Security <ul style="list-style-type: none"> followed, reviewed, updated, and tested regularly prohibit retention team to lead response activities responsibilities in advance (eg. communications) identification, containment, eradication, recovery, and follow-up ensure chain of custody, impartiality, and follow evidence Security <ul style="list-style-type: none"> performed on each business case prior to allocation of resources security by design security interfaces developed according to industry standards Security <ul style="list-style-type: none"> risks are documented, followed, reviewed, and updated regularly meet or exceed organizations' security policy regularly test to demonstrate evidence of compliance risks are identified, mitigated, and reviewed regularly Security <ul style="list-style-type: none"> test and patching approved, followed, reviewed, and updated regularly test prior to and following production launch test regularly to ensure current OS and application levels tests are regularly conducted as part of a program and documented according to organizational policy capabilities must be remediated through patching or compensating controls

Defensible | What are they after?



Identify the Crown Jewels

It is critical to invest in resources that identify and classify the most viable information assets, and to determine where they are and who has access to them.

Defensible | Good hygiene



- Identify your most sensitive data to protect – where does it reside, why do they want it?
- Take a defensive in depth approach
- Keep antivirus definitions up-to-date and scanning regularly
- Patch your operating system and software
- Use strong authentication practices
- Be wary of social engineering and don't open emails / attachments from unknown sources

Defensible | Strong compliance



- Utilize a cyber framework to manage your overall security program
- Network with Industry peers to explore best practices
- Document policies and procedures
- Assign responsibilities to hold everyone accountable
- Measure program results and communicate results – continuous improvement



TELUS' Journey

Defensible and Beyond

Target breach | Inflection point for TELUS



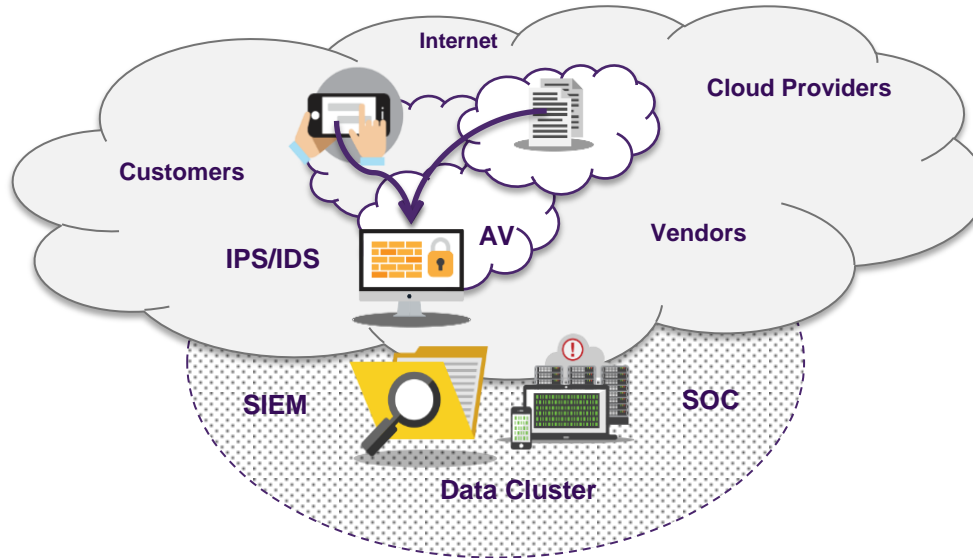
- 2013**
 - July 5 ● BlackPOS advertised for sale in Russian underground site for \$1000
 - Dec 18 ● Target breach story breaks, American Express and U.S. Secret Service publicly confirm Target breach
 - Dec 19 ● Target publicly confirms breach of credit and debit card information, 40 million customers data breached
- 2014**
 - Jan 10 ● Target publicly revises number of customers affected to worst case number of 110 million
 - Mar 5 ● CIO resigns
 - Mar 26 ● Banks file lawsuit against Trustwave and Target
 - Apr 23 ● Cyber Risk insurance providers take action to increase premiums and reduce coverage limits
 - May 5 ● CEO resigns

TELUS Security | Core beliefs

- Security is about **quantifying and reducing risk**
- It's also about **enabling innovation**
- **Technology alone** will not make you secure
- Your frontline employees can be your **weakest link** or one of your **most advanced detection systems**

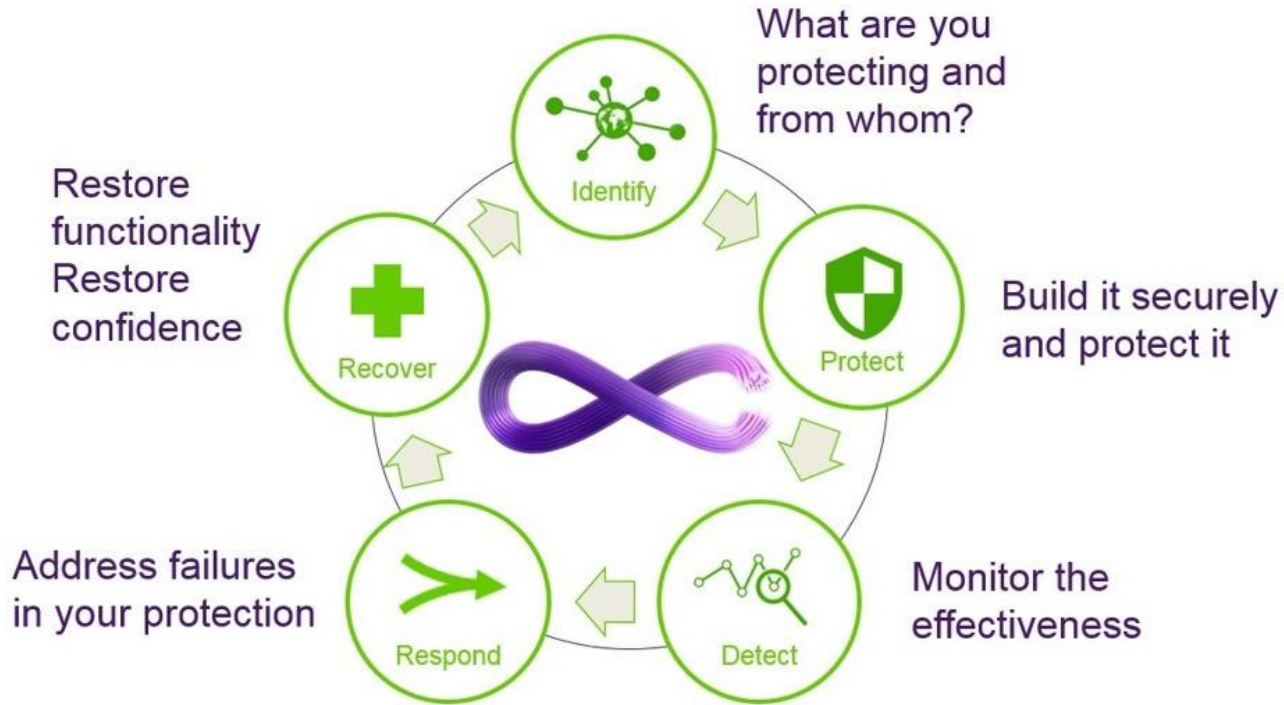


TELUS ecosystem | Beyond defensible



Risk Based Security – Measurable Outcomes

Security ecosystem





Protect the Anchor Client

Cyber security analytics

Expand the use of predictive data, analytics and threat intelligence to detect and respond to cyber threats.

Secure-by-Design

Ensure that security is included in the fundamental design of all TELUS services throughout the full lifecycle.

Governance, Risk & Compliance

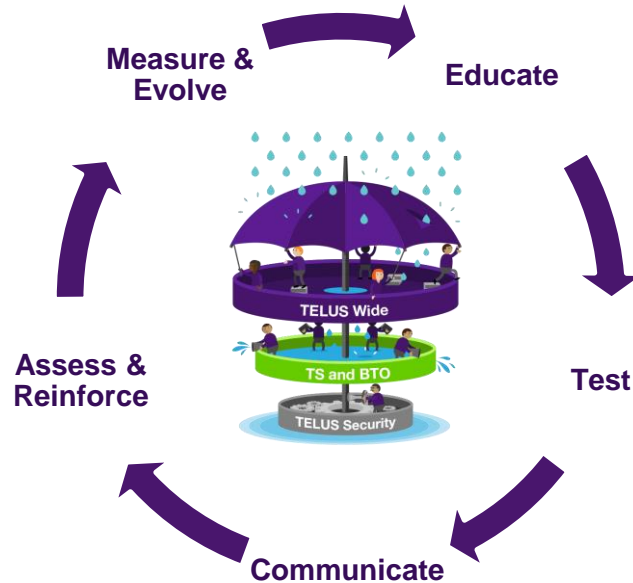
Improve the protection of TELUS assets leveraging people, process & technology informed by sound risk management.

Utilize the experience and expertise to improve solutions for our customers.

Protecting the Anchor Client | How we do Secure by Design



A consistent approach to communication and training



Enhancing our security community and building a strong first line of defense

Phishing Simulations | Practice makes perfect(ish)



Why?

- The phishing threat landscape is continuously evolving as threat actors change who they are targeting and how
- To convert a potential weakness into our first line of defence
- Help secure your organization by educating Team Members on how to be secure at both at work and at home

How?

- **TEST** - send out frequent simulations of increasing difficulty to continuously engage and challenge Team Members
- **ASSESS** - Track and assess Team Member click through and report rates
- **TRAIN** - Provide additional information and training to teams or individuals with low scores
- **EVOLVE** – Use real world data and simulation results to evolve, focusing on areas of weakness

Continuously developing our Culture of Security



Reference Materials

Ensure security policy and guidelines are readily available to all Team Members



Real-world Events

Produce articles reporting on global security incidents as they happen



Engaging Topics

Use personally engaging security topics to engage and educate Team Members



At Work = At Home

Encourage Team Members to use security best practices both at work and at home

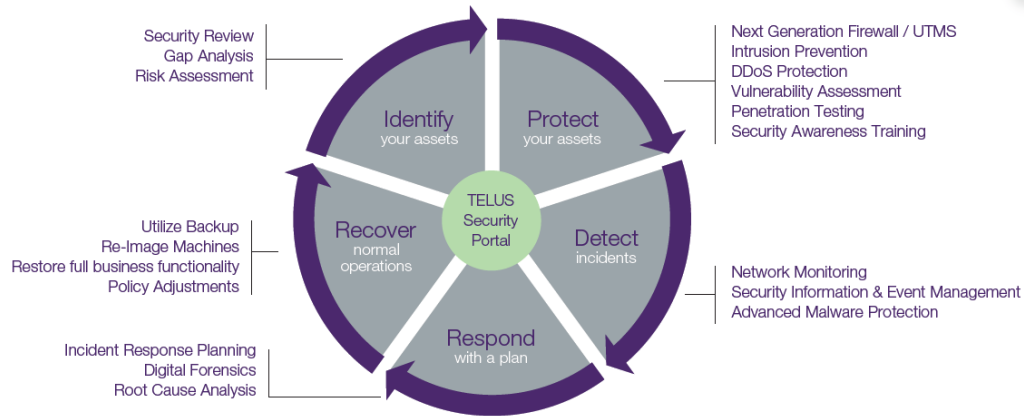


Reporting

See Something?
Say Something

What we do for our Clients

How TELUS supports our customers' security ecosystems



Our Methodology



First Step | TELUS Defensible Security Gap Assessment

TELUS Security



Defensible Security Gap Assessment

In the course of its daily business, information systems collect, process, store, and selectively disseminate a significant amount of confidential information and therefore incur a wide range of responsibilities with respect to protection and availability of the confidential data, including:

- Appropriate controls around access to information;
- Integrity of business information and transactions;
- Availability of business information systems and continuity of business operations;
- Ensuring business information is managed in compliant with all application legislative requirements and contractual obligations.

In view of this TELUS provides security expertise to perform a Security Gap assessment aimed at enabling our clients to determine the robustness of existing processes, controls, and standards to safeguard the confidentiality, integrity, availability and privacy of enterprise and customer information. The assessment will identify and quantify the maturity levels of our client's internal processes, gain visibility into the current security posture and identify gaps that may exist relative to the Defensible Security Framework for Public Sector Organization. This gap analysis will identify potential control deficiencies within the environment relative to requirements described in the Defensible Security Framework to assess the extent of the corresponding risks and provide recommendation actions on achieving compliance.

This assessment is used to compare an organization's current cybersecurity activities with those outlined in the Framework and provide a prioritized plan to address gaps. An organization may find that it is already achieving the desired outcomes, thus achieving compliance to the requirements set out in the Framework. Conversely, an organization may determine that it has opportunities to (or needs to) improve. The organization, supported by the security expertise of TELUS, can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is over-investing to achieve certain outcomes. The organization can use this information to prioritize resources to strengthen other cybersecurity practices.

The Security assessment exercise shall determine the client's compliance to the following areas as required in the Framework:

<ul style="list-style-type: none">• Asset Management & Disposal• Change Management• Incident Management• Business Continuity Plan (BCP)• Disaster Recovery Plan (DRP)• Backup & Retention• Logging & Monitoring• Physical Security & Visible Identification• Security Incident Response• Information Security Policy	<ul style="list-style-type: none">• Information Security Program• Information Security Classification• Criminal Record Checks• Security Awareness Program & Course• Vendor Security Requirements• Access Control• Defence in Depth for Endpoints and Networks• Security Governance• Vulnerability Management and Patching
---	---

The Province of British Columbia Defensible Security for Public Sector Organizations Framework



Strategy & Planning



Core Security Infrastructure



Testing Security



Monitoring & Analytics



Incident Response



- Embrace expert advice from a third party to baseline your cyber security posture (hygiene & compliance) and identify gaps
- Third party assessments are a quick way to understand and communicate organizational deficiencies and to recommend actions for achieving compliance



Thank You

 **TELUS**[®] | Business