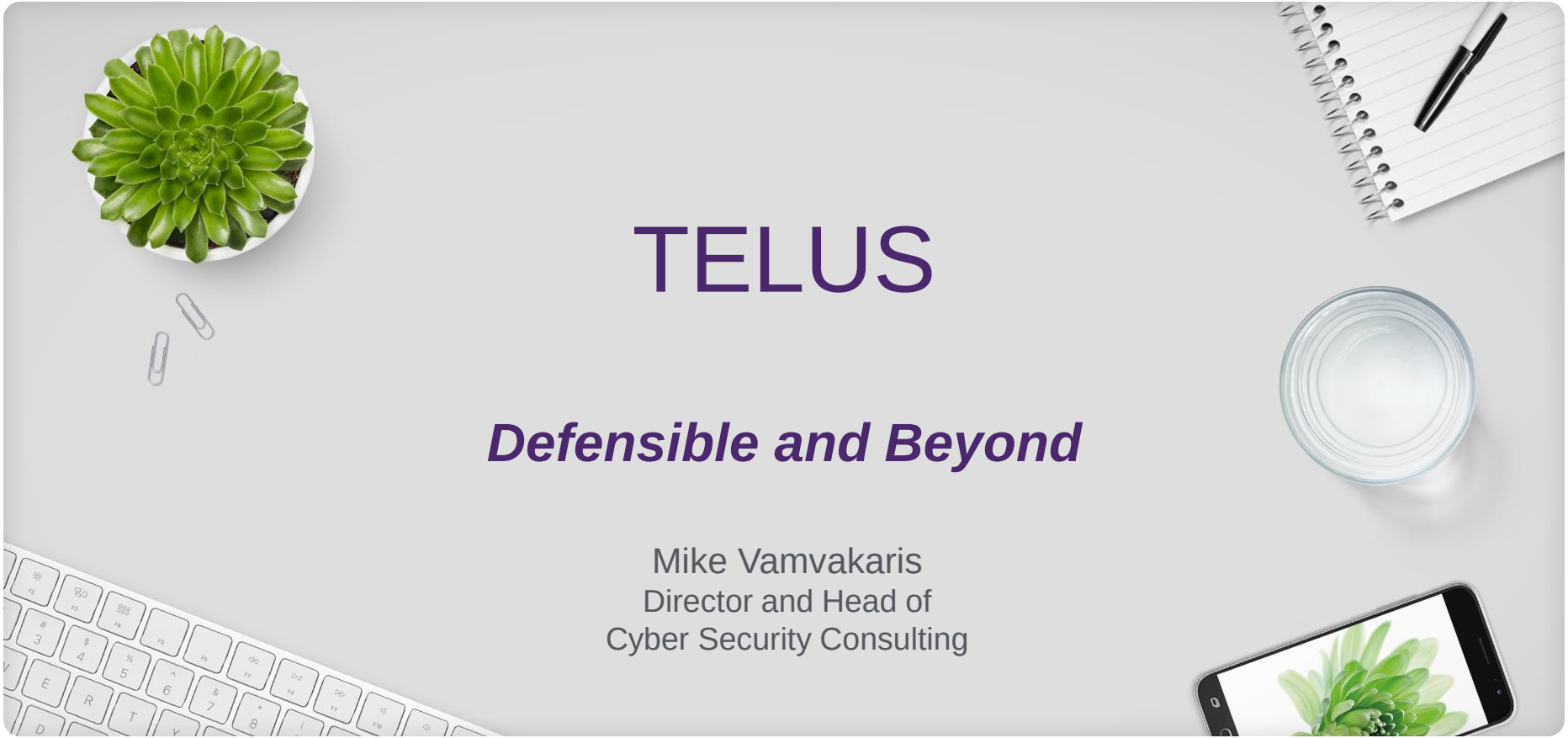


TELUS

Defensible and Beyond

Mike Vamvakaris
Director and Head of
Cyber Security Consulting

November 2017

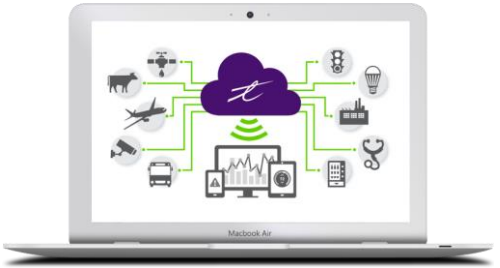
TELUS Business

Digital transformation brings many benefits…

Communication and Collaboration

Autonomous and Artificial Intelligence (AI)

Internet of Things (IoT)



…it also brings new risks

160% *YoY growth in cybersecurity incidents in Canada*

85% *Organizations reported being victim of a phishing attack*

49% *Businesses fell victims to cyber ransom attacks in 2016*

38% *Organizations have systems/controls for advanced threats*

54K *IT skills gap in Canada in 2016: key areas include IT operations, security and programming*

Source: IDC, Cisco, Hootsuite, Gartner, Statista

TELUS Business

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

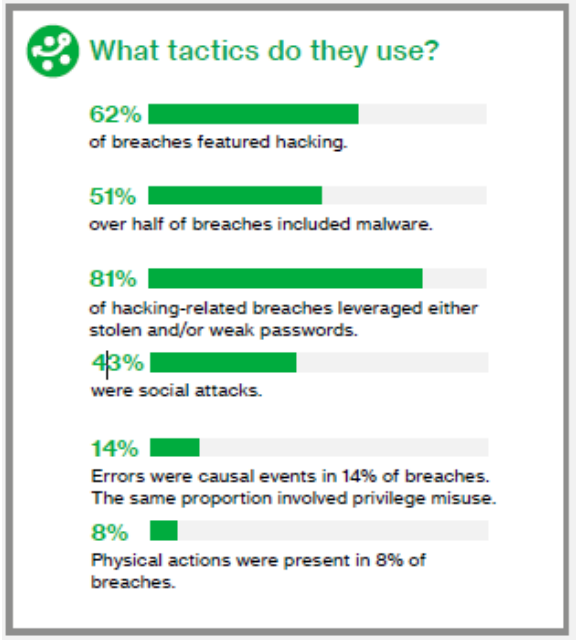
The costs of single cyber attacks are **increasing**

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

TELUS Business

How are they getting in? | Emerging threats

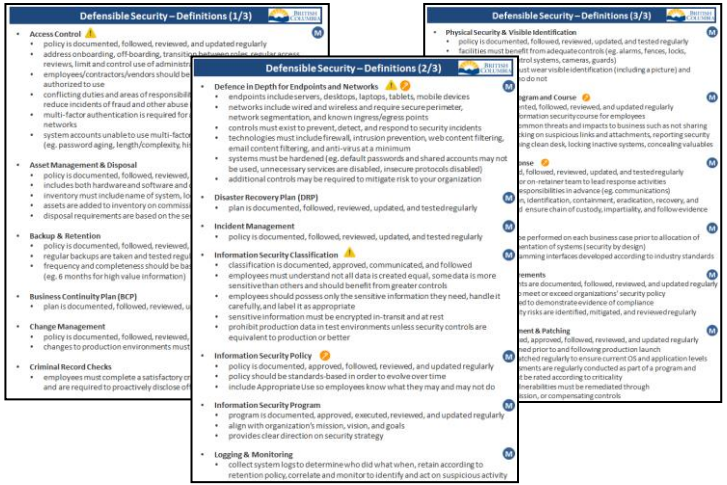
- Ransomware
- Phishing attacks
- DDoS attacks
- IoT / weak passwords
- Hardware / Firmware targets
- Mobile device attacks
- Social media fake ads
- Hacking personal devices – smartphones, tablets



Source: 2017 Verizon DBIR

TELUS Business

Why Defensible? | No organization is immune to attack



TELUS Business

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.

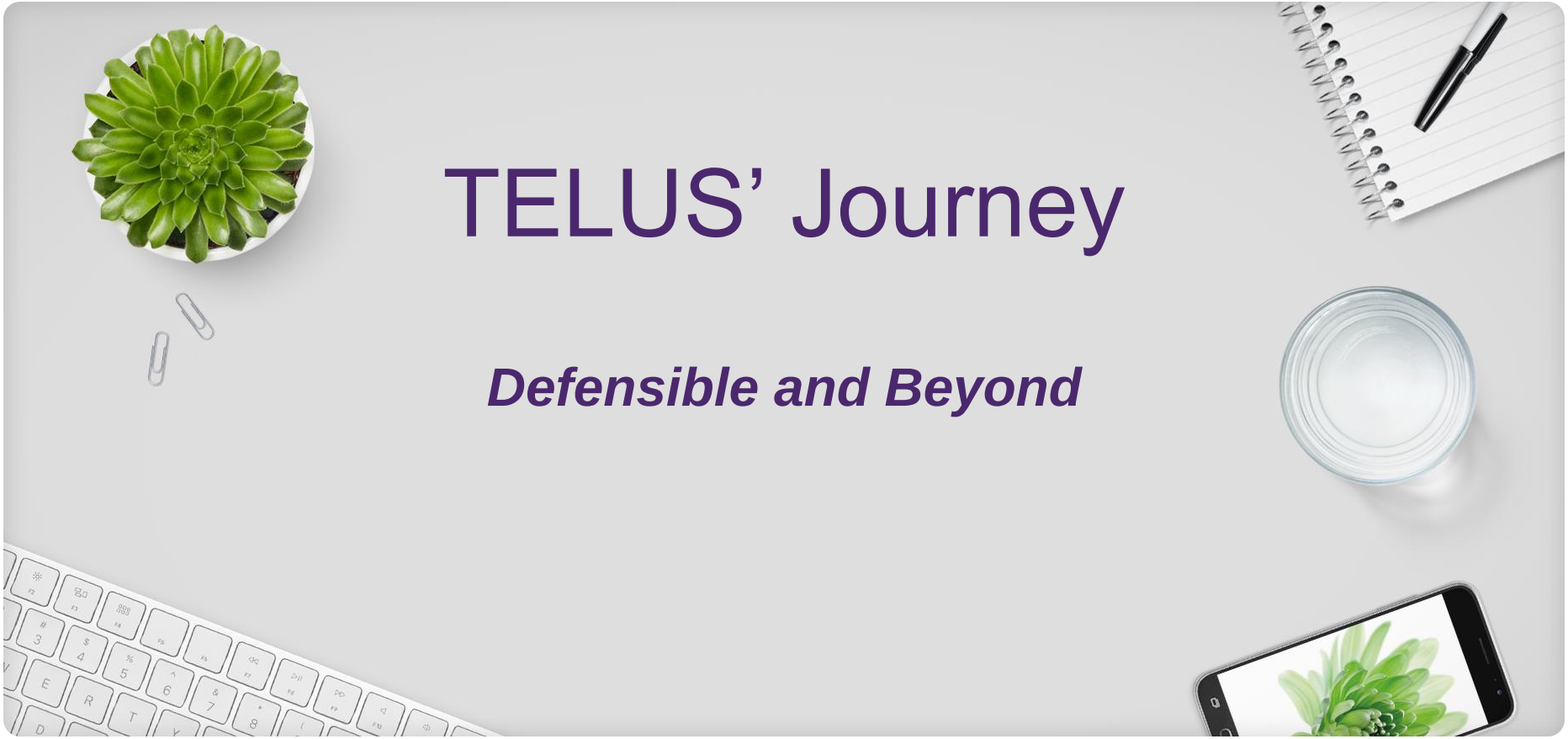
Defensible | Good hygiene

- 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 Business



TELUS' Journey

Defensible and Beyond

TELUS | Business

Target breach | Inflection point for TELUS

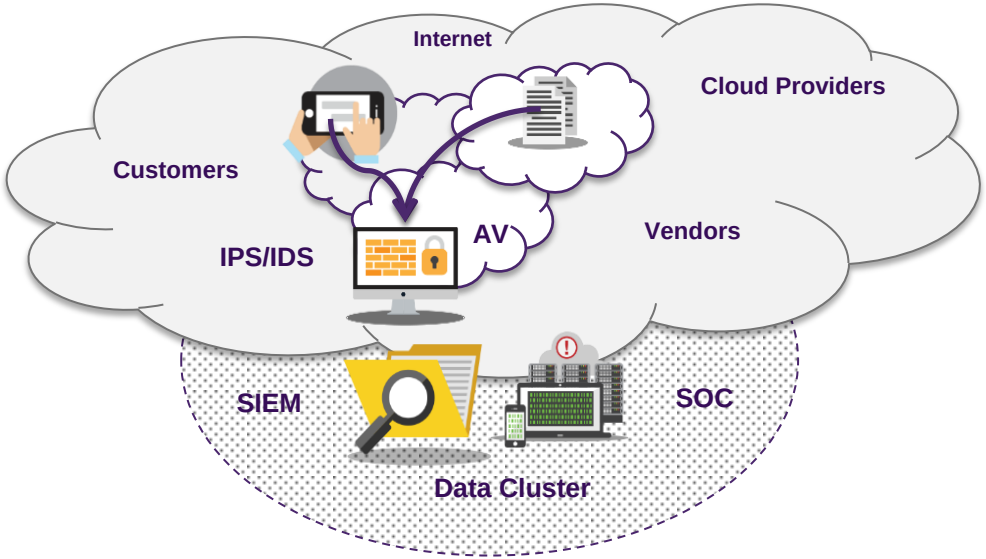
2013	July 5	BlackPOS advertised for sale in Russian underground site for $1000
	Dec 18	Target breach story breaks, American Express and U.S. Secret Service publically confirm Target breach
	Dec 19	Target publically confirms breach of credit and debit card information, 40 million customers data breached
2014	Jan 10	Target publically 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 Business

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**

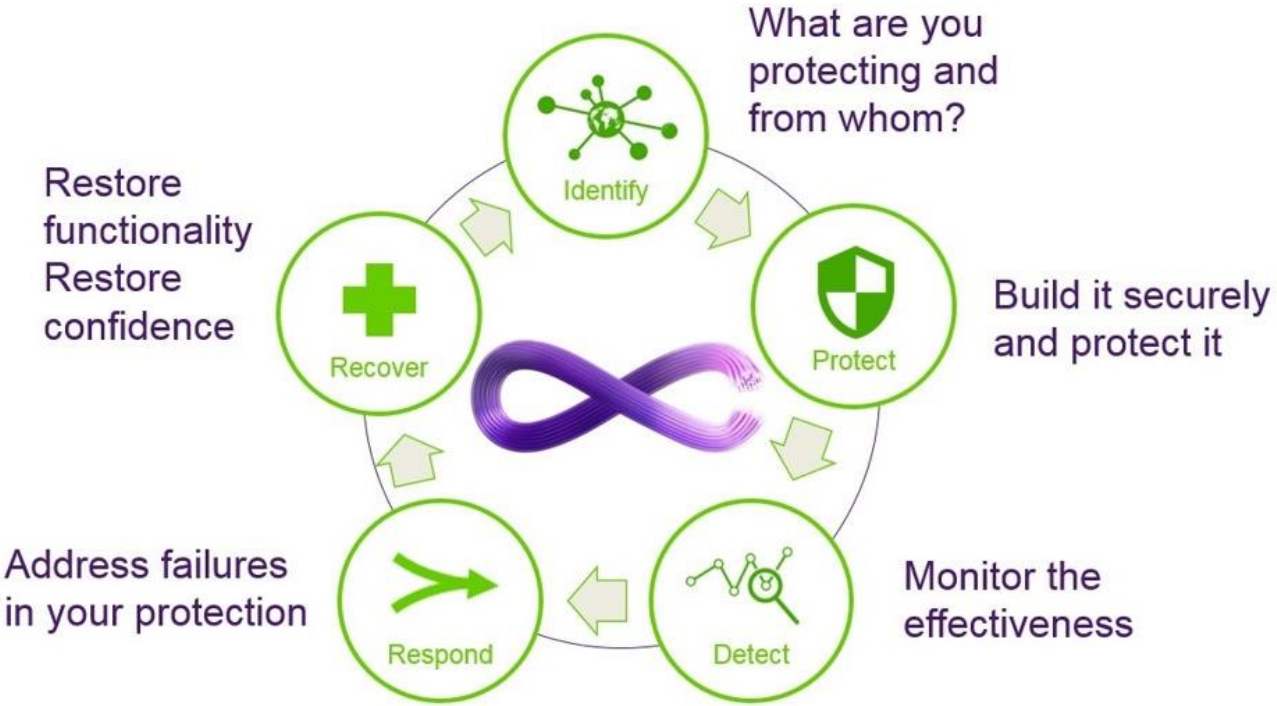
TELUS ecosystem | Beyond defensible



Risk Based Security – Measurable Outcomes

TELUS Business

Security ecosystem



TELUS | Crown jewels

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

TGRC-Sherpa
TELUS Governance, Risk and Compliance solutions

Sherpa

TELUS GRC tool to track projects, risks & mitigation timelines

Security Library

- Supporting documents for our corporate policy and risk tolerance

NIST Checklist

- List of approved systems to meet NIST functions (e.g. use Corp. LDAP)
- Mappings to other control and certification standards

Threat Model Library

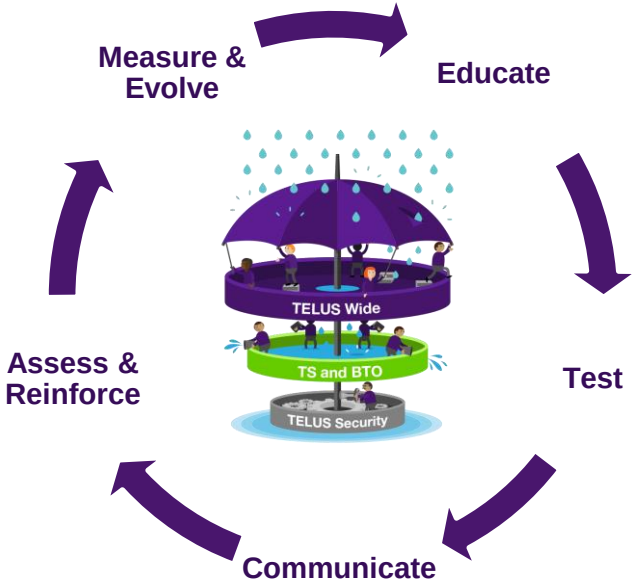
- Standard requirements for standard scenarios (e.g. web server in a DMZ)

Security Expert

Once basic security has been approved

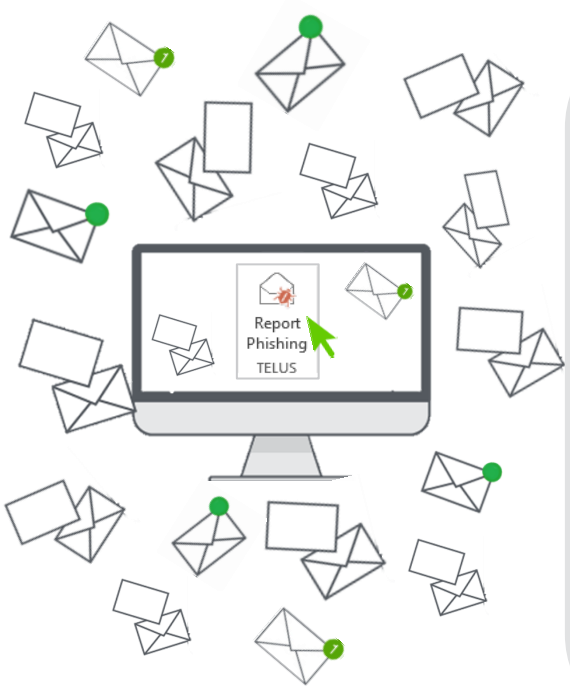
TELUS Business

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

TELUS Business

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

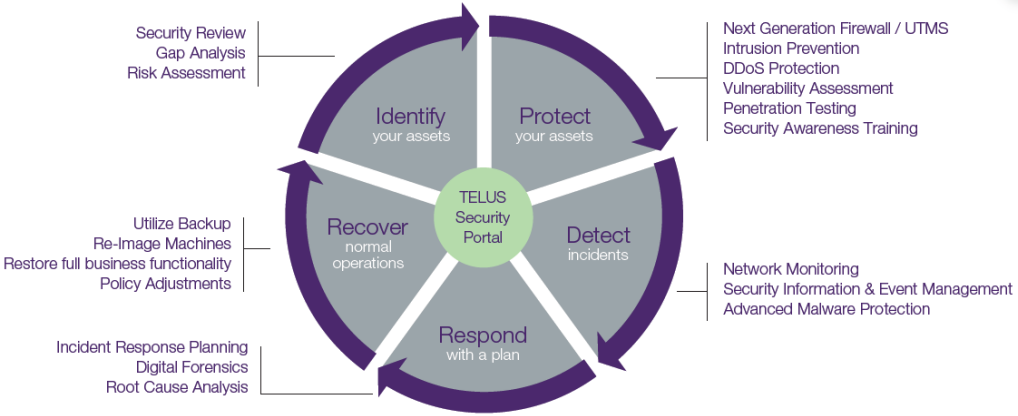
Encourage Team Members to use security best practices both at work and at home

Reporting

See Something? Say Something

What we do for our Clients

How TELUS supports our customers' security ecosystems



Our Methodology

TELUS Business

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**[1] 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 overinvesting to achieve certain outcomes. The organization can use this information to reprioritize 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:

- 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
- 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

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

TELUS | Business

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

TELUS | Business


Thank You
TELUS
Business