Strategies for the Eroding Network Perimeter: Defend the Perimeter or Retreat to Higher Ground

Kenneth Haertling

VP & Chief Security Officer

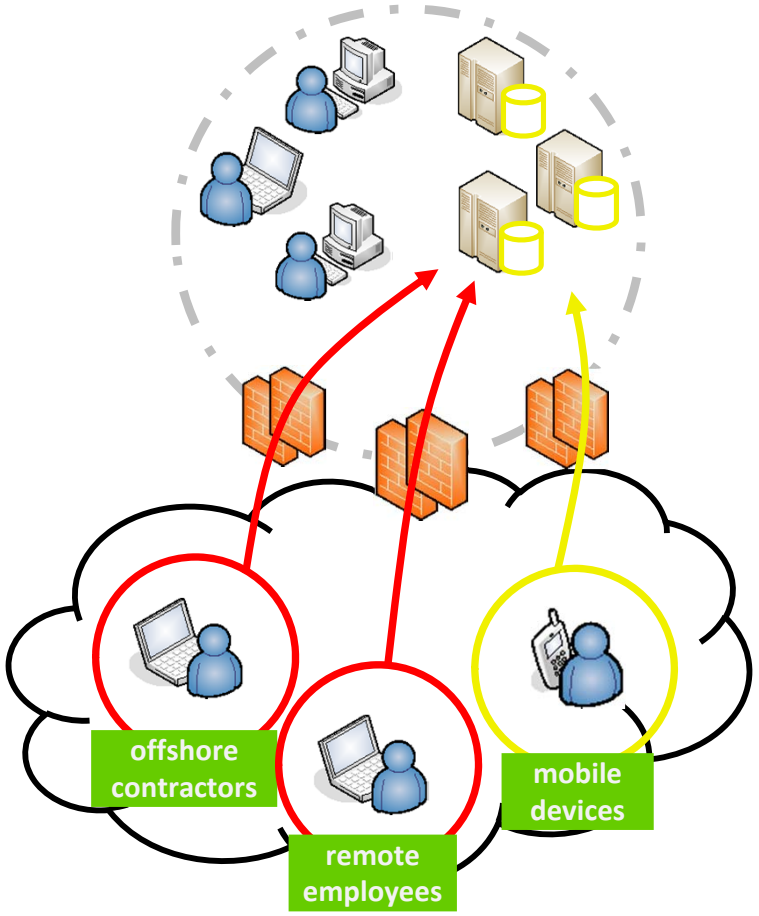
TELUS Corporation

Session ID: TECH-402

Session Classification: Intermediate

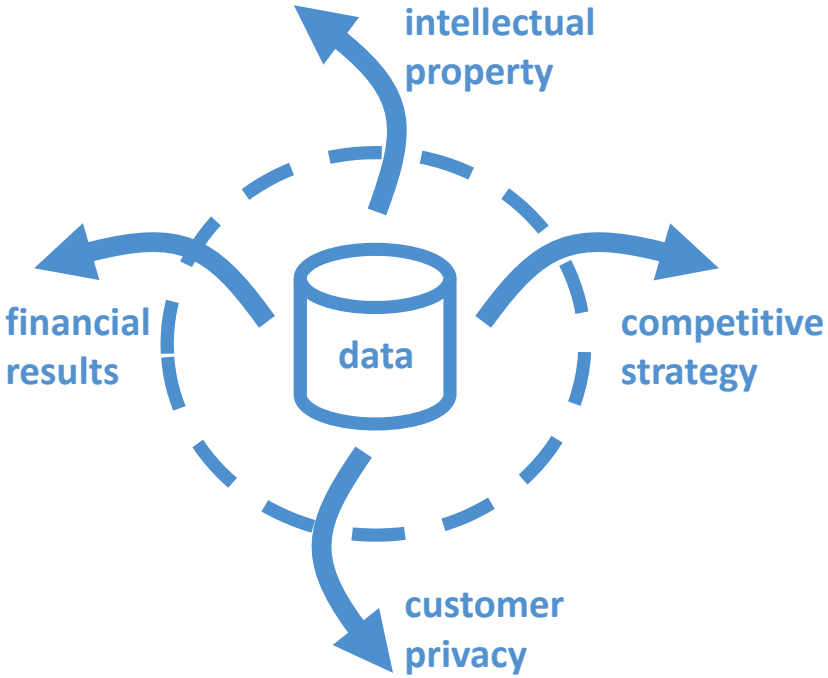
Introduction

- fundamental shift over last decade in perimeter traffic
  - ten years ago, IP-based firewalls were sufficient
    - limited holes punched in firewall
    - employees worked autonomously within physical enterprise environment
  - today, IP-based firewalls are no longer sufficient
    - numerous holes in firewall
    - shift in employee work styles with “mobile workers”
- network perimeter is eroding at a rapid pace
  - employee network is no longer trusted
  - employee space is little more than a DMZ
- presentation objectives
  - possible solutions to address
  - lessons learned
  - key takeaways



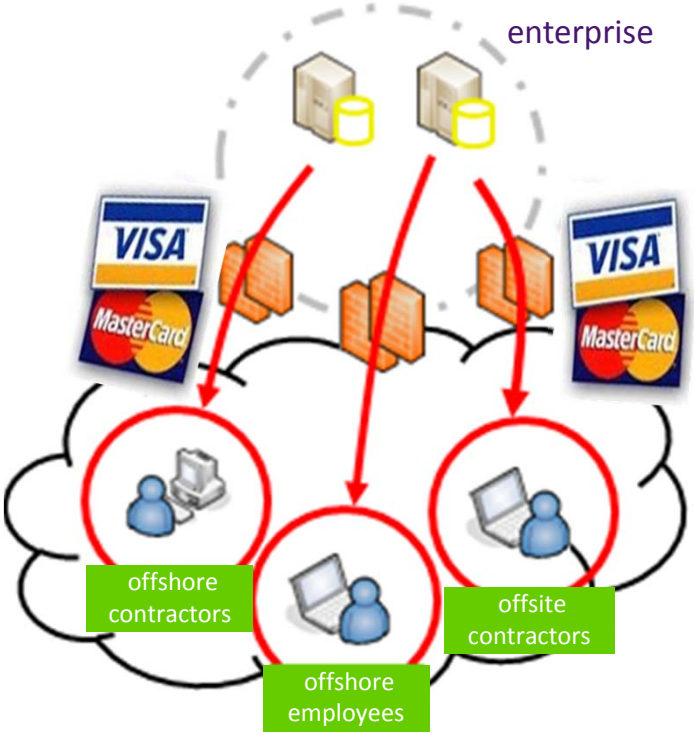
Threat landscape

- areas of impact (due to porous network perimeter)
  - intellectual property
  - competitive strategy
  - financial results, insider trading info
  - bid/procurement selection data
  - customer privacy
  - service assurance/product integrity
- cost of impact
  - financial
  - brand/reputation
  - sustained competitive advantage
- tension between prevention vs. cost
  - risk management focus
    - prevent
    - mitigate
    - accept



Outsourcing/Offshoring

- offshoring is a key portion of business at TELUS



- impact to network perimeter
  - offshore requires access to data to function
  - offshore requires tools to be productive
  - results in more holes punched in already porous perimeter

- challenging to secure data
  - sensitive data shifting outside enterprise control
    - customer phone numbers
    - credit card numbers
  - data exposed both local and offshore

Mobile Employees

- objective to have employees work from wherever whenever

TELUS Employees	Past	Present	Future
office	95%	60%	**30%**
mobile	5%	30%	**40%**
home	0%	10%	**30%**

- key drivers
  - corporate real estate cost
  - high salaries for urban areas
  - attracting new young talent

- impact to network perimeter
  - employees require access to data to function
  - employees require tools to be productive
  - results in more holes punched in already porous perimeter

Mobile Devices

- industry mobile trends
  - shift from purpose-built enterprise devices (Blackberry) to consumer built devices (Android, Apple)
  - difficult to prevent employees from bringing devices from home
  - effective mobile device management is difficult
- TELUS implementation of BYOS (Smartphone)
  - wireless carriers must be progressive in adoption of technology
  - joint use work and personal device intermixing personal and private data
  - arming employee base with devices to pull our data

TELUS Role	Subsidy	Refresh	Monthly $
back office	$350	2 yrs	$15
sales	$850	1 yrs	$15

- Tablet evolution
  - deeper level of file manipulation (building/editing docs)
  - access to enterprise applications/SaaS
  - hop between home DSL, home WiFi, public WiFi, corporate network, corporate WiFi and telco network
  - for all purposes a laptop requiring full remote access

Tsunami of Ingress/Egress traffic

- information overload: trends at TELUS

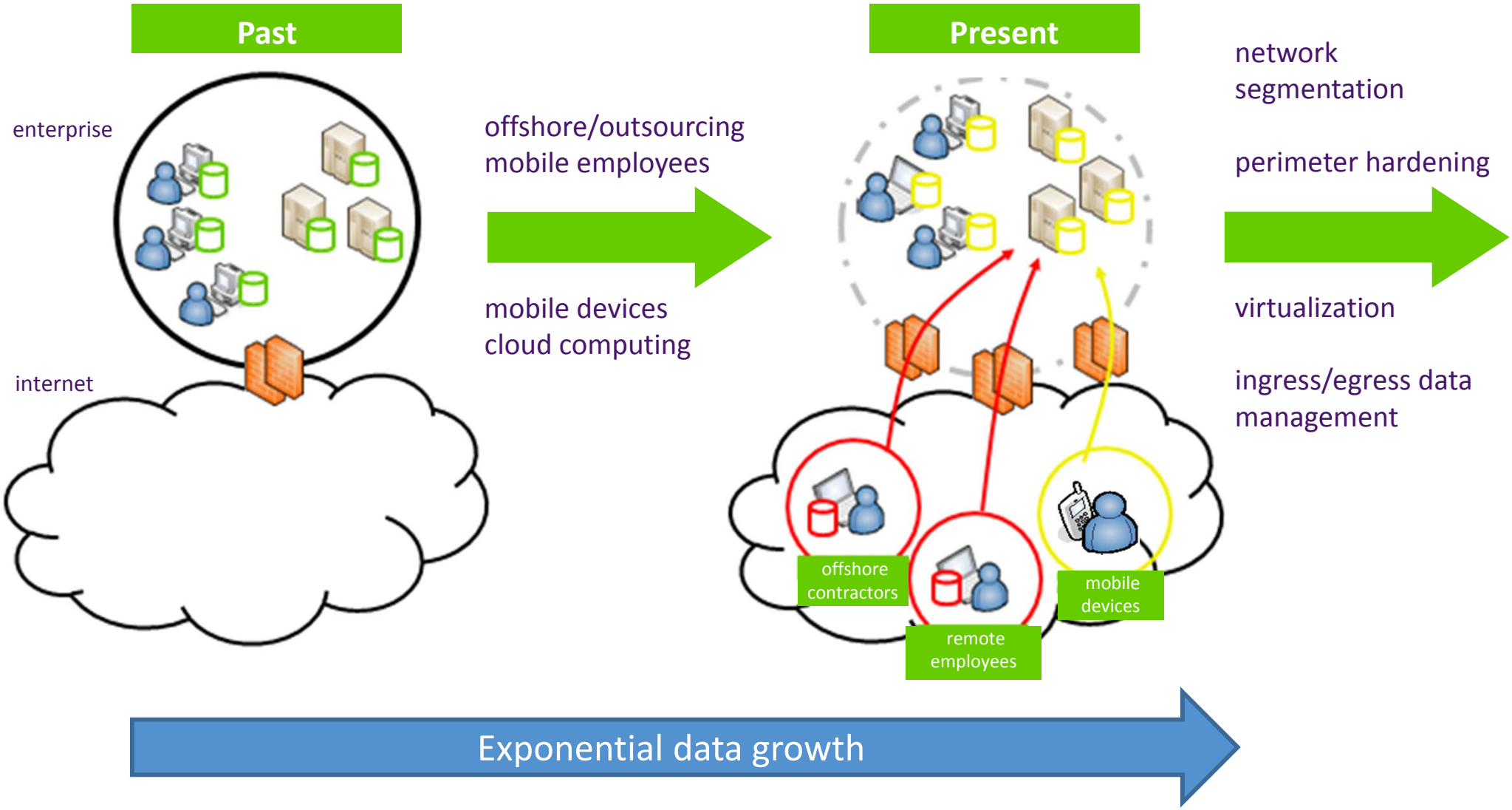
Item	Increase	Drivers
ingress/egress points	20x	web portals, document sharing, VPN tunnels, mobile device data, virtualization
data passing through perimeter	100x	outsourcing, work from home, mobile devices
security inspection points	5x	firewalls, IDS/IPS, content filtering, DLP

- security inspection tool evolution
  - honeymoon
  - climbing the mountain
  - reach exhaustion and give up

- impossible task of synthesizing tsunami of data
  - how to tune security devices to clearly call out actionable security response

- proliferation of encryption blinding security inspection

Eroding Network Perimeter

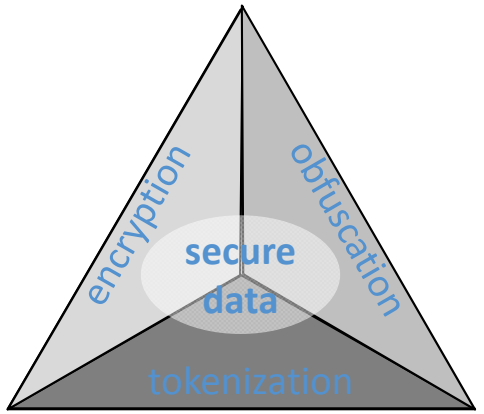


Understand Your Data

- understand problem space
  - most security solutions are poor proxies for data security
  - understand your data, users, and behaviour
  - 10% of users leverage 80% of companies highly sensitive data
- original approach
  - secure all data everywhere (reactive)
  - variety of technical solutions (encryption, data erasure/destruction, etc)
  - challenging to protect data at rest on less than trusted networks
- new surgical approach
  - proactive posture
    - data awareness (understand threat, data, people)
    - data classification (understand vital data)
  - surgical application of data security controls is key
  - recognize key projects, initiatives with robust security
  - consider specific solutions
    - encryption
    - tokenization
    - obfuscation

PCI analogy

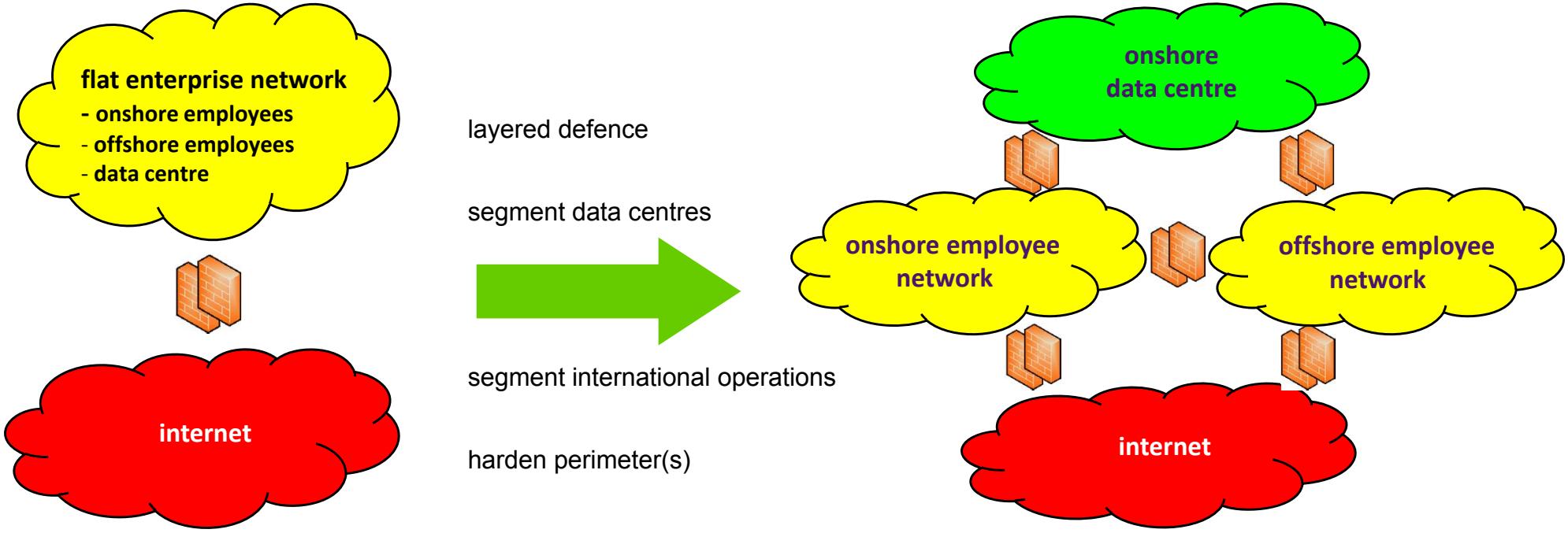
- failed when tried to include entire enterprise network in scope
- failed when tried to make extensive use of encryption
- succeeded in surgical focus on credit card data and use of tokenization



Network Segmentation

- typical enterprise networks today are flat
  - no segmentation between data centre and employee environments
  - most enterprises are hard on the exterior, squishy in the middle
- can no longer trust internal employee network
  - ensure segmentation in right areas with DMZ approach
  - employees, data centres, international/subsidiaries

Consider the following…
70% of enterprises have a flat network and do not segment employees from data centres
22% of hacks come from insiders
IT adoption



Perimeter Hardening (Where)

- traditional perimeter/approaches

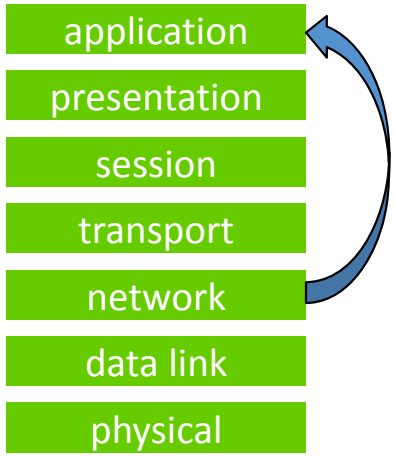
Percentage of companies leveraging:	
IP-based firewalls	99%
intrusion prevention	65%
content filtering	30%
data loss prevention	15%
application-based firewalls	10%

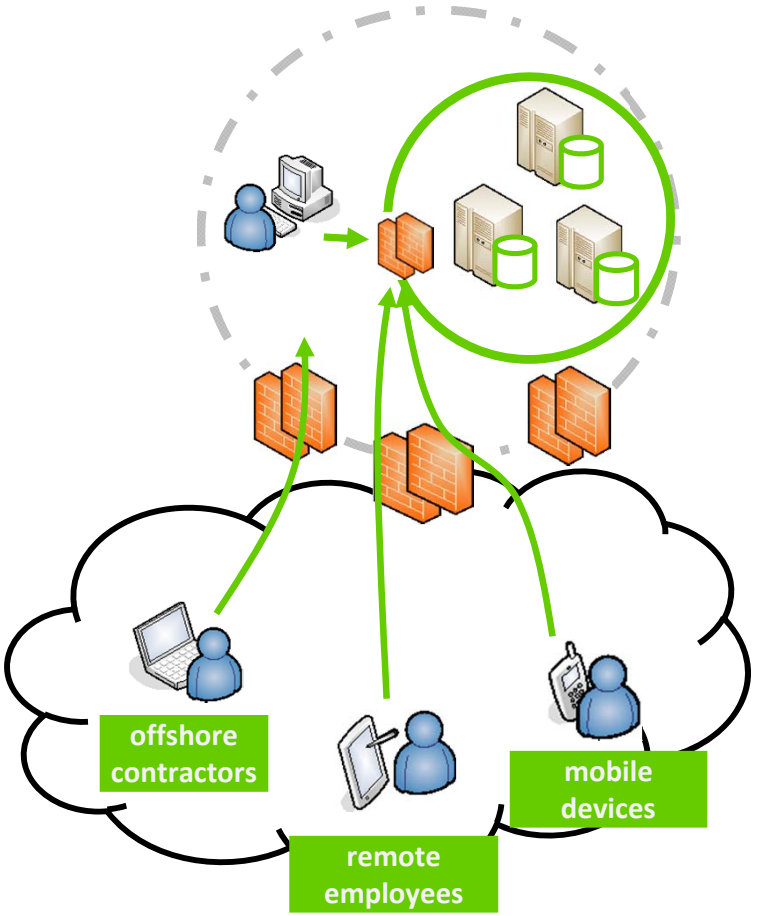
hard, crunchy exterior
soft, gooey centre

- double down, harden traditional perimeter
  - extremely difficult and expensive to do well
  - default approach – assess from risk perspective
  - appropriate for high value enterprise environment (ie. DoD, Nuclear power plant)
  - may be fighting a losing battle
- harvest perimeter
  - consider risk appetite
  - cost constraints
  - finite dollars protecting most critical infrastructure

Perimeter Hardening (How)

- data centre perimeter
  - optimal point for robust data security controls
- need to move up the stack
  - right layer of inspection (layer 3 vs. layer 7)
  - true data inspection
- technology
  - IP-based firewalls
  - application based firewalls
  - IDS/IPS
  - content filtering
  - data loss prevention
  - DDoS prevention
  - SIEM





- advantages of higher layer defences
  - fine-grained policy management
  - application visibility and application control, anomaly detection
  - control over users and data content
  - fused intelligence and policy

Virtualization of Desktops

- popularity of desktop virtualization
  - 62% of companies use virtualization
  - enabler for at home, offshore
  - key control for asset and data security

TELUS	2009	2011	2013
virtualized desktops	500	8,000	16,000
supported employees/ contractors	1000	16,000	32,000
total employees/ contractors	35,000	40,000	45,000

- merits of virtualization
  - protect the data
    - data never at rest outside the data centre
    - provide views into data
  - protecting identity/credentials is vital
    - assume being key-logged
    - authenticate by clicking on-screen keyboard

- lessons learned
  - in 2010, virtualization was thought to be the solution
  - virtualization is effective for only 85% of the job functions and required applications

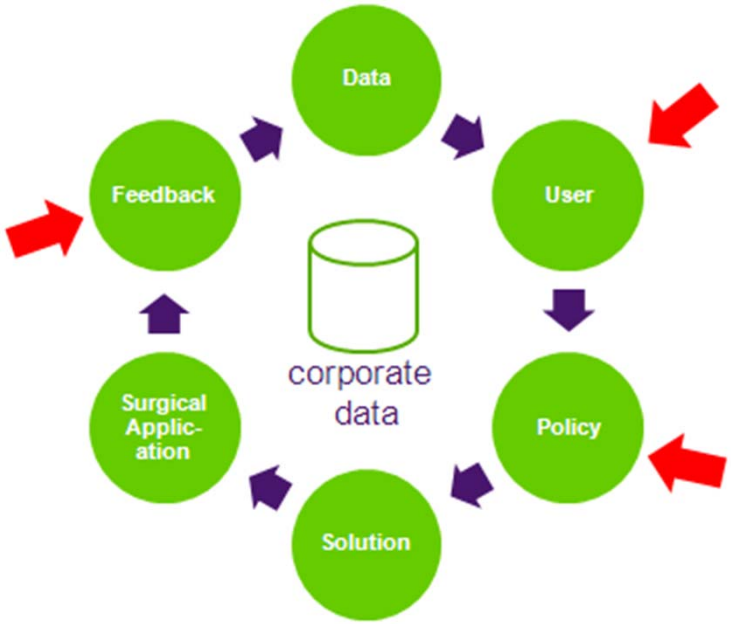
Managing Ingress/Egress Traffic

- key themes
  - reduce total volume of data
  - only inspect high risk data
  - ensure data not encrypted at inspection points
- analogy of department store
  - review every customer through front door (employee enterprise network)
  - only inspect customers in electronics & jewellery counters (data centre)
- risk acceptance and prioritization
  - DMZ view of employee enterprise network
  - protect the crown jewels of the data centre
- surgical application of operations resources
  - focus on data centre traffic
  - feedback loop: detect ► respond ► tuning ► repeat

Item	Decrease
data passing through perimeter	1/10
ingress/egress points	1/5
security inspection points	1/2

Lessons Learned

- surgically apply security controls
  - understand your data, users, and behaviour
  - 10% of users control 80% of critical data
- partner with business on offshoring
- enable employees to bring their own devices
  - wireless ambassadors
- device management is a poor proxy for data security
- virtualization is not the magic bullet that solves everything
  - virtualization works 85% of the time
- overload of security event data which is largely unactionable



Takeaways - Apply

Short term: (30 days)

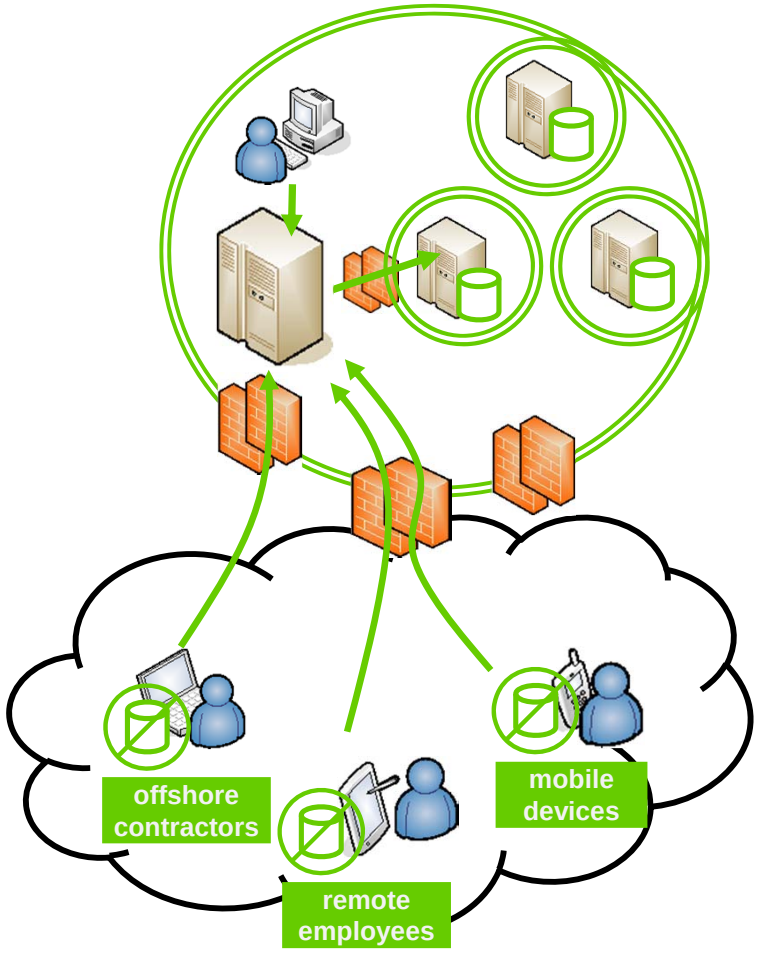
- traditional network perimeter becoming less effective
  - don't trust your enterprise network and view it as a DMZ
- embrace new technology
  - don't manage devices, manage the data security

Medium term: (60-90 days)

- virtualization
  - ensure data is never at rest outside the data centre
- surgical application of controls
  - focus hardening on data centre
  - focus at appropriate layer of OSI model

Long term: (90-180 days)

- layered defence
  - segment your data centres
- know and manage your data
  - deploy SIEM and robust security controls at data centre perimeter



Questions?

Contact information

Kenneth Haertling

VP & Chief Security Officer

TELUS Corporation

kenneth.haertling@telus.com

Links

2011 Rotman-TELUS Security Study http://www.rotman.utoronto.ca/securitystudy/