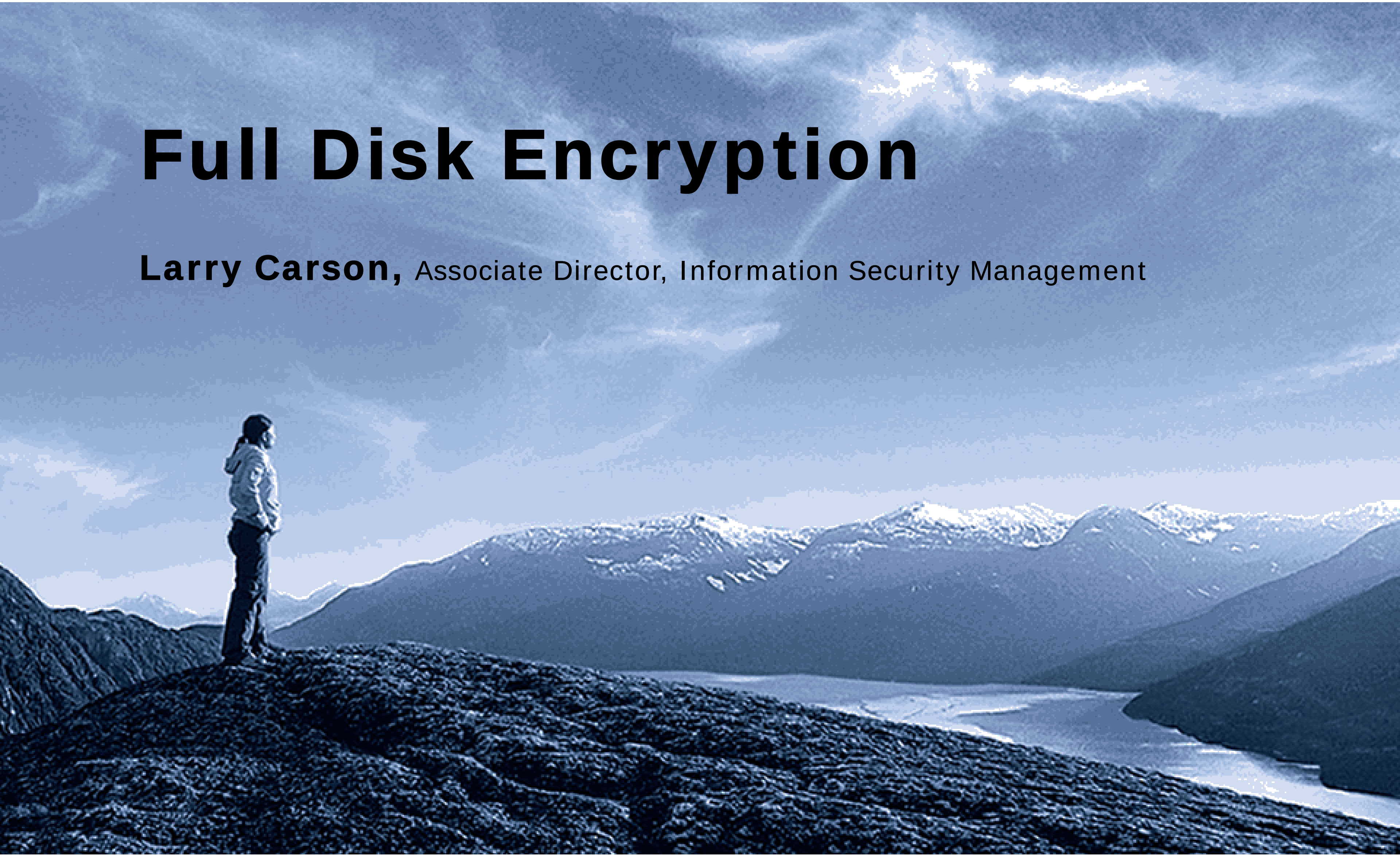
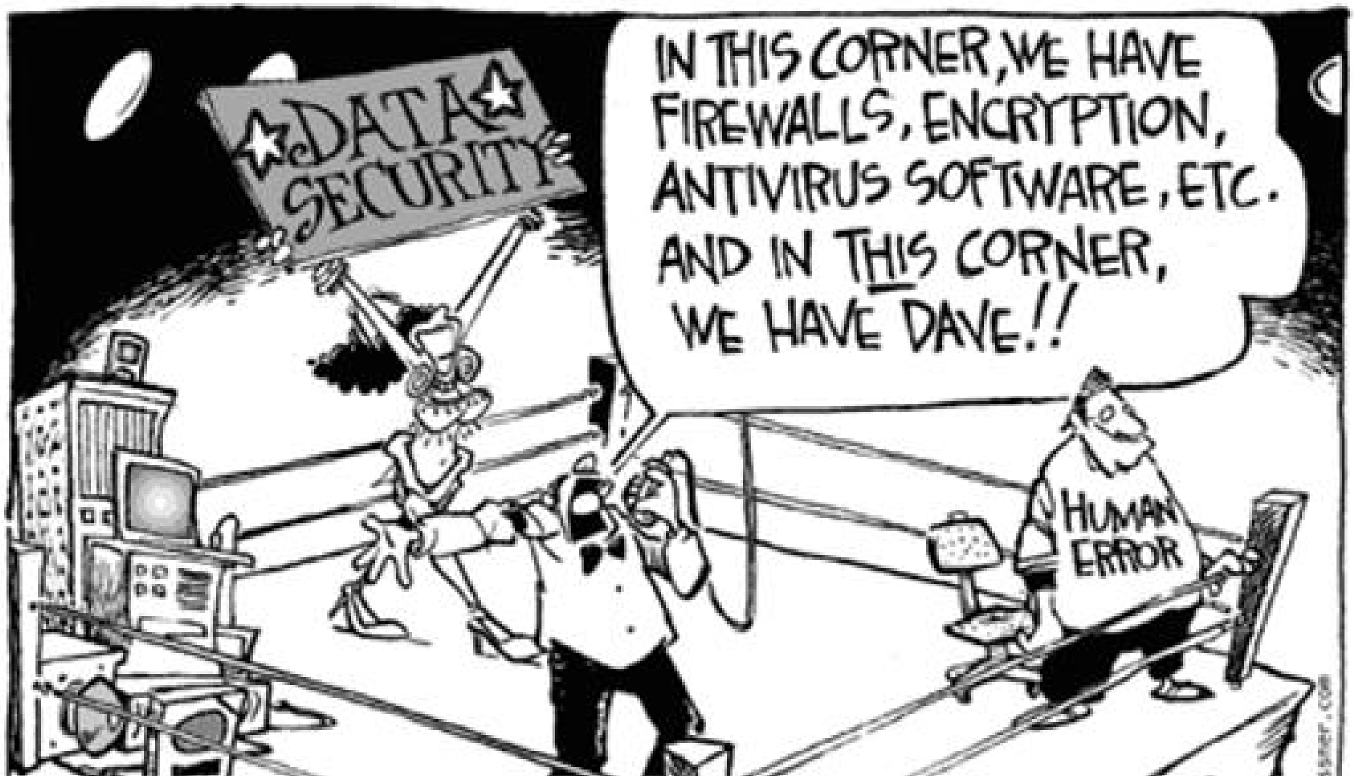
INFORMATION TECHNOLOGY
engage • envision • enable

Full Disk Encryption

Larry Carson, Associate Director, Information Security Management



What Security Really Looks Like at UBC


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

News-worthy Security Incidents

VGH Loss of 450 medical records via Resident laptop & USB drive
Lost/stolen at Toronto airport
(Late Sep 2011)

UVic Loss of 11,845 employee records incl. banking info
Stolen USB stick
(Jan 2012)

Costs: Est $500K-$1M

UBC Laptop Loss & Recovery with 50,000 records
Stolen from vehicle
(Feb 2012)

Elections Ontario ~2.4 million voter records lost
(2) Unencrypted USB sticks
(Apr 2012)

Human Resources and Skills Development (HRSD) 583,000 student Loan records
lost external hard drive
(Jan 2013)

Costs: $270K+

Canada's Privacy Commissioner's Office 800 employee records
lost external hard drive
(Feb 2014)

BC Ministry of Education Loss of 3.4 million student records
External hard drive missing
(Sep 2015)

UBC Loss of 160 student records
TA Laptop stolen from campus
(Oct 2015)

Definition of Personal Information

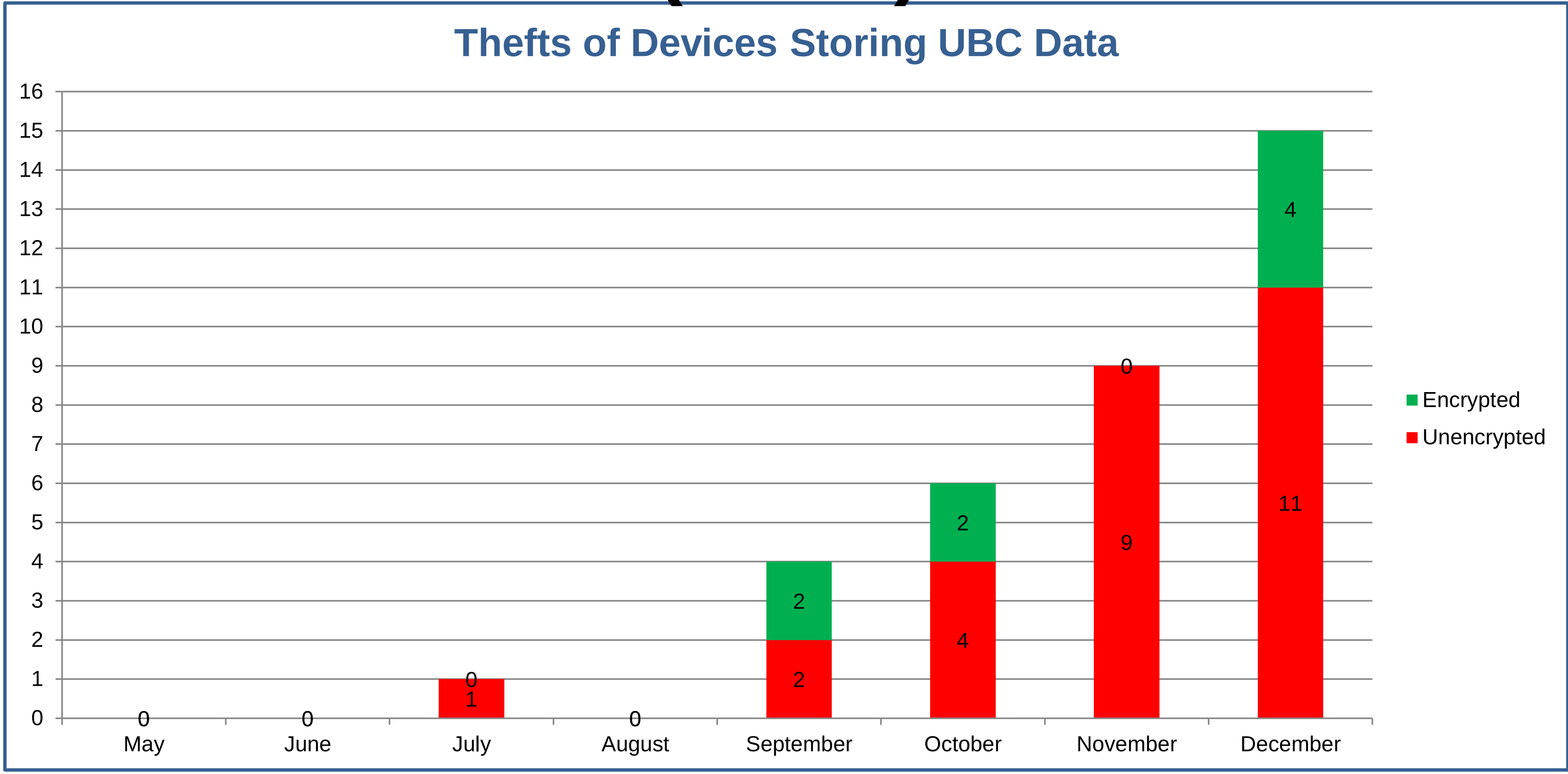
“**recorded information** about an **identifiable individual**, not including **contact information**”

Contact information: “**information to enable an individual at a place of business to be contacted**, including the name, position name or title, business telephone number, business address, business email or business fax number of the individual”

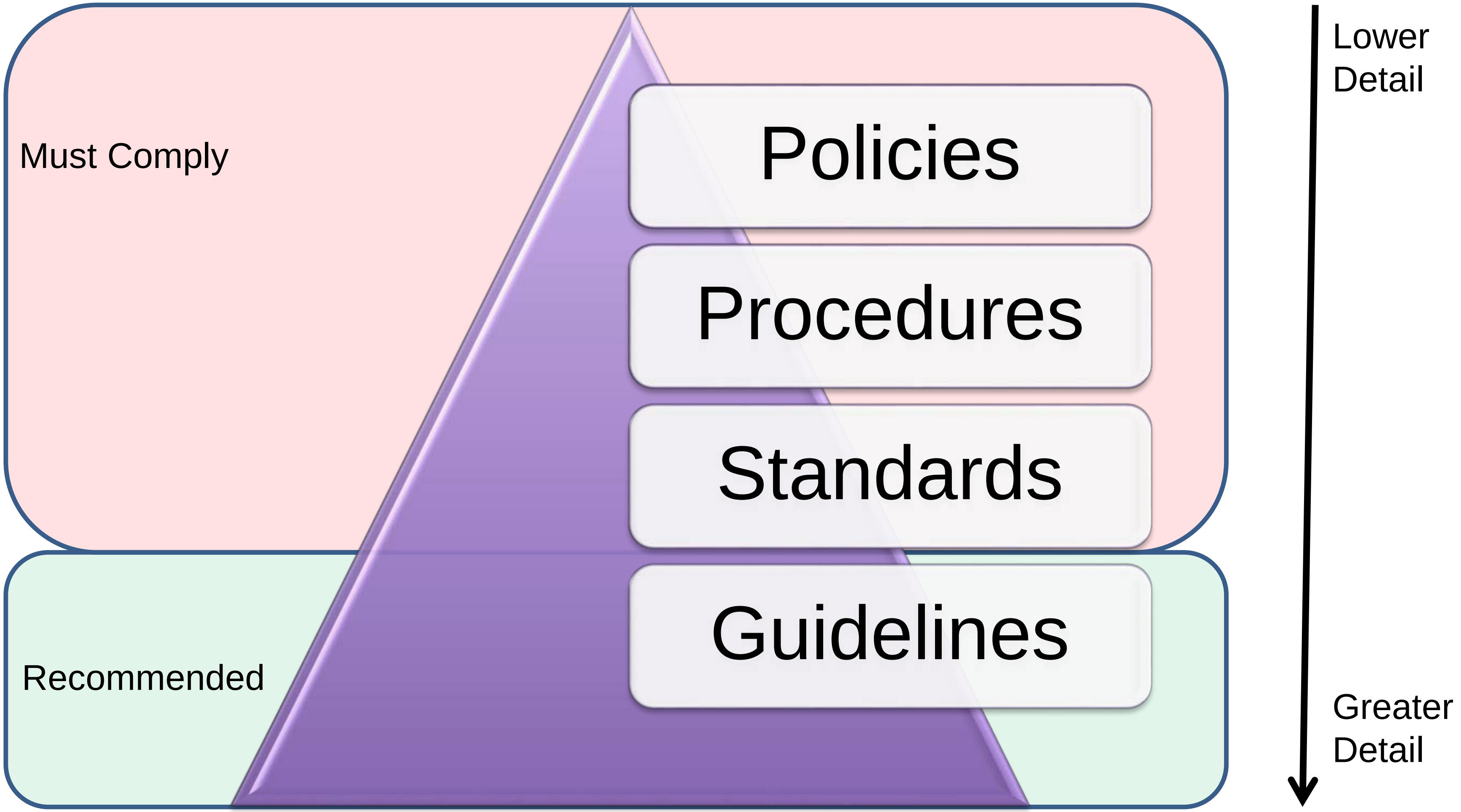
10 Things You Must Know about Privacy

1. You must be able to identify personal information
2. Your regular work activities are not private
3. Embarrassment is not a valid reason to withhold records
4. Use privacy notifications to collect personal information
5. Retain personal information for at least one year
6. Disclose personal information on a “need to know” basis
7. Protect personal information using reasonable security
8. Don’t store personal information outside Canada
9. Report privacy breaches promptly
10. Do privacy impact assessments for new projects

UBC Recent Stats on Thefts (2015)



Policies, Procedures, Standards & Guidelines



Must Comply

Recommended

Policies

Procedures

Standards

Guidelines

Lower Detail

Greater Detail

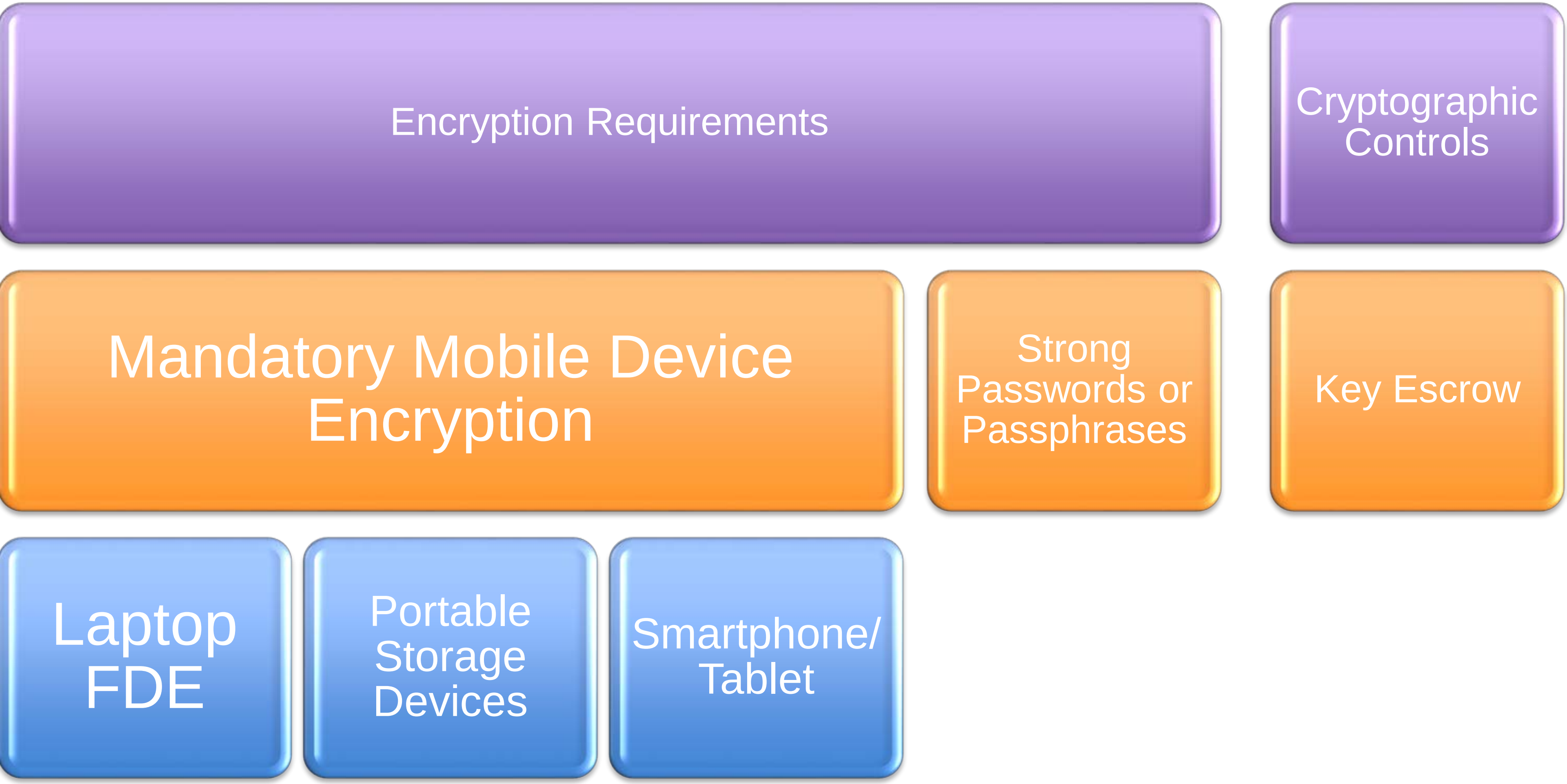
UBC Policies & Standards

#104 Acceptable Use and Security of UBC Electronic Information and Systems (June 2013)
http://cio.ubc.ca/securitystandards

(10) Standards for All Users

(11) Management & Technical Standards

21 Standards
Incl. Cryptographic Controls



Encryption Requirements

Cryptographic Controls

Mandatory Mobile Device Encryption

Strong Passwords or Passphrases

Key Escrow

Laptop FDE

Portable Storage Devices

Smartphone/ Tablet

Device Encryption: What to Encrypt

Encrypt Laptops – UBC provides a commercial solution at no cost

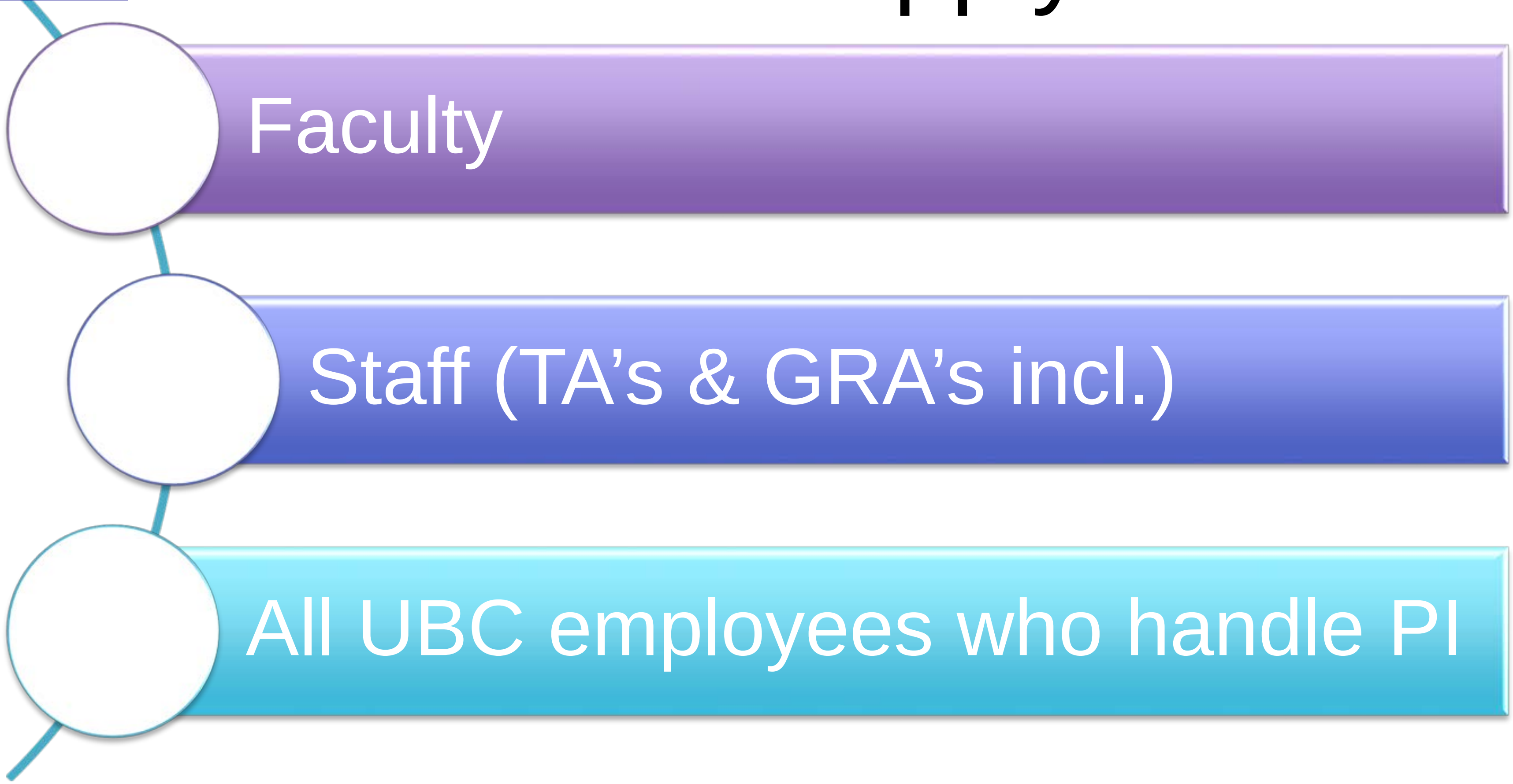
- Encrypt High risk desktops/servers

Encrypt Storage Devices

Encrypt Smartphones/Tablets

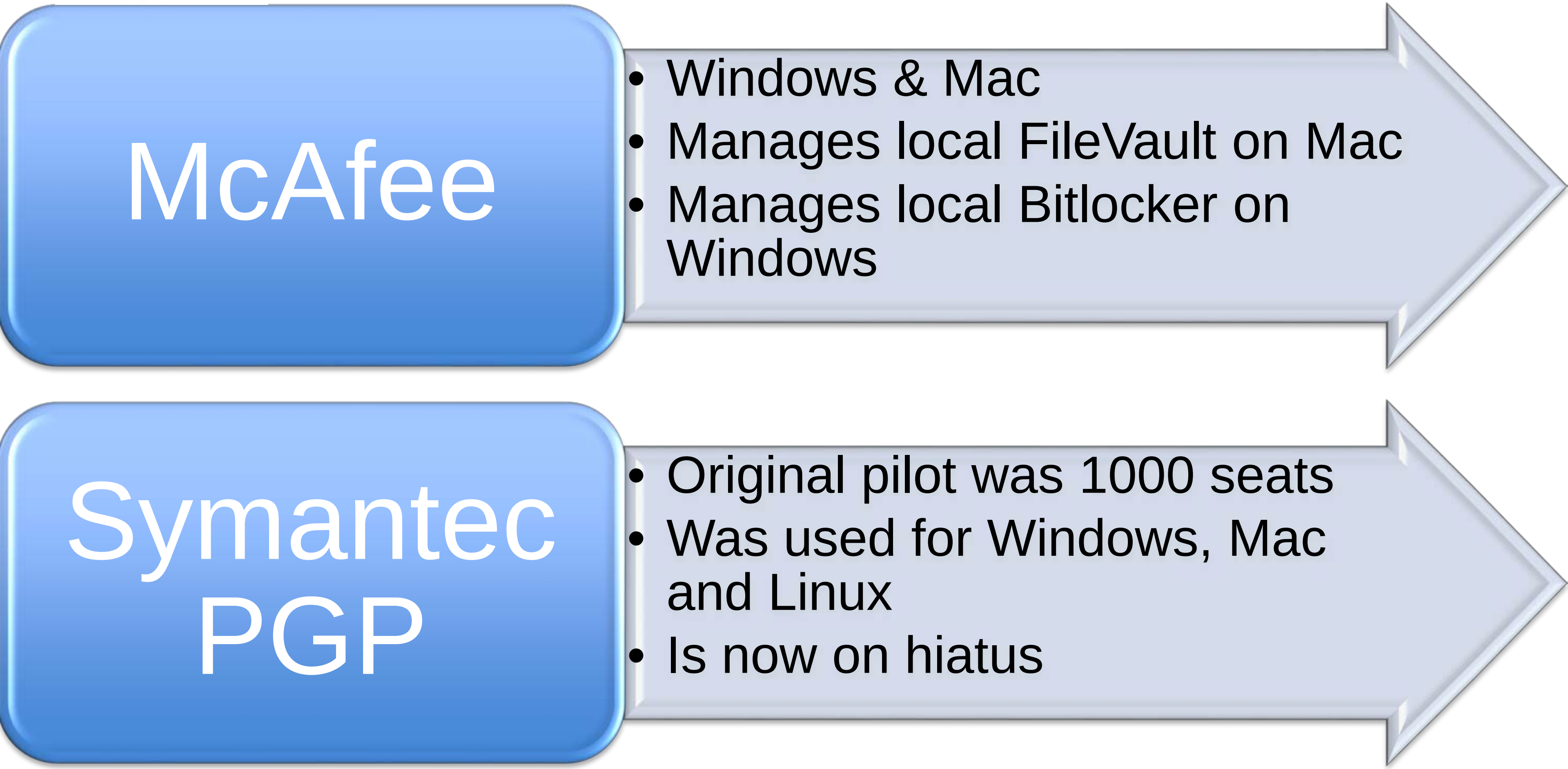
Encrypt Personally owned devices if they contain UBC Personal Information (PI)

Device Encryption: Who does it apply to?



- Faculty
- Staff (TA's & GRA's incl.)
- All UBC employees who handle PI

Tools



McAfee

- Windows & Mac
- Manages local FileVault on Mac
- Manages local Bitlocker on Windows

Symantec PGP

- Original pilot was 1000 seats
- Was used for Windows, Mac and Linux
- Is now on hiatus

Devices

To be encrypted

- Laptops – all with PI
- Desktops that are high risk (traffic, data, etc.)

Exemptions

- Eligible: laptops that do not/will not contain PI. e.g. certain research lab computers

Other Considerations

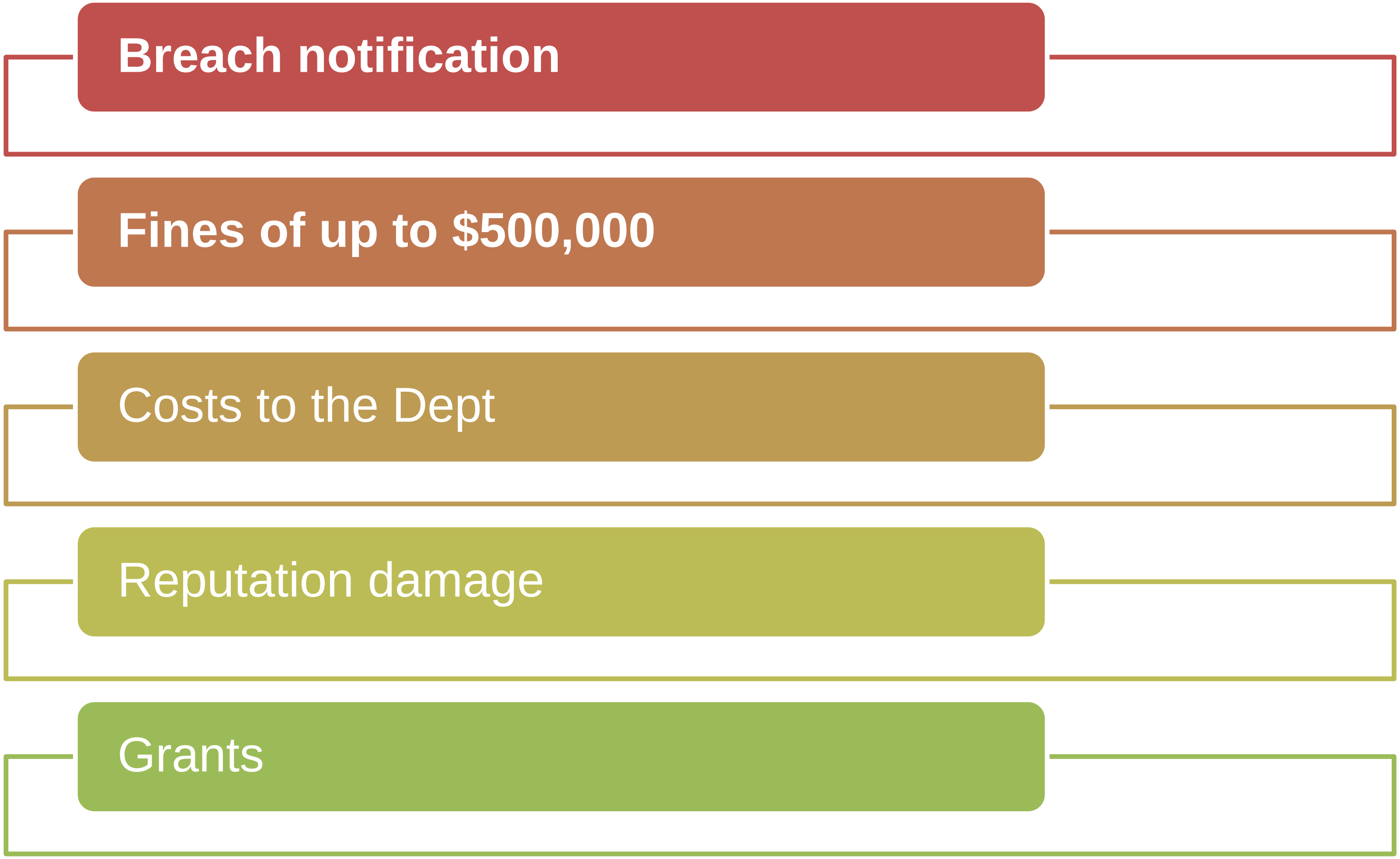
Don’t keep more data than you need on mobile devices

- Delete records that aren’t needed
  - Backup old class lists to network shares and delete them from the device
- Delete Columns/Attributes that aren’t needed – especially high sensitivity PI (PHI, SIN, DoB, etc.)

Don’t store class lists in the cloud (e.g. DropBox, Google, etc.)

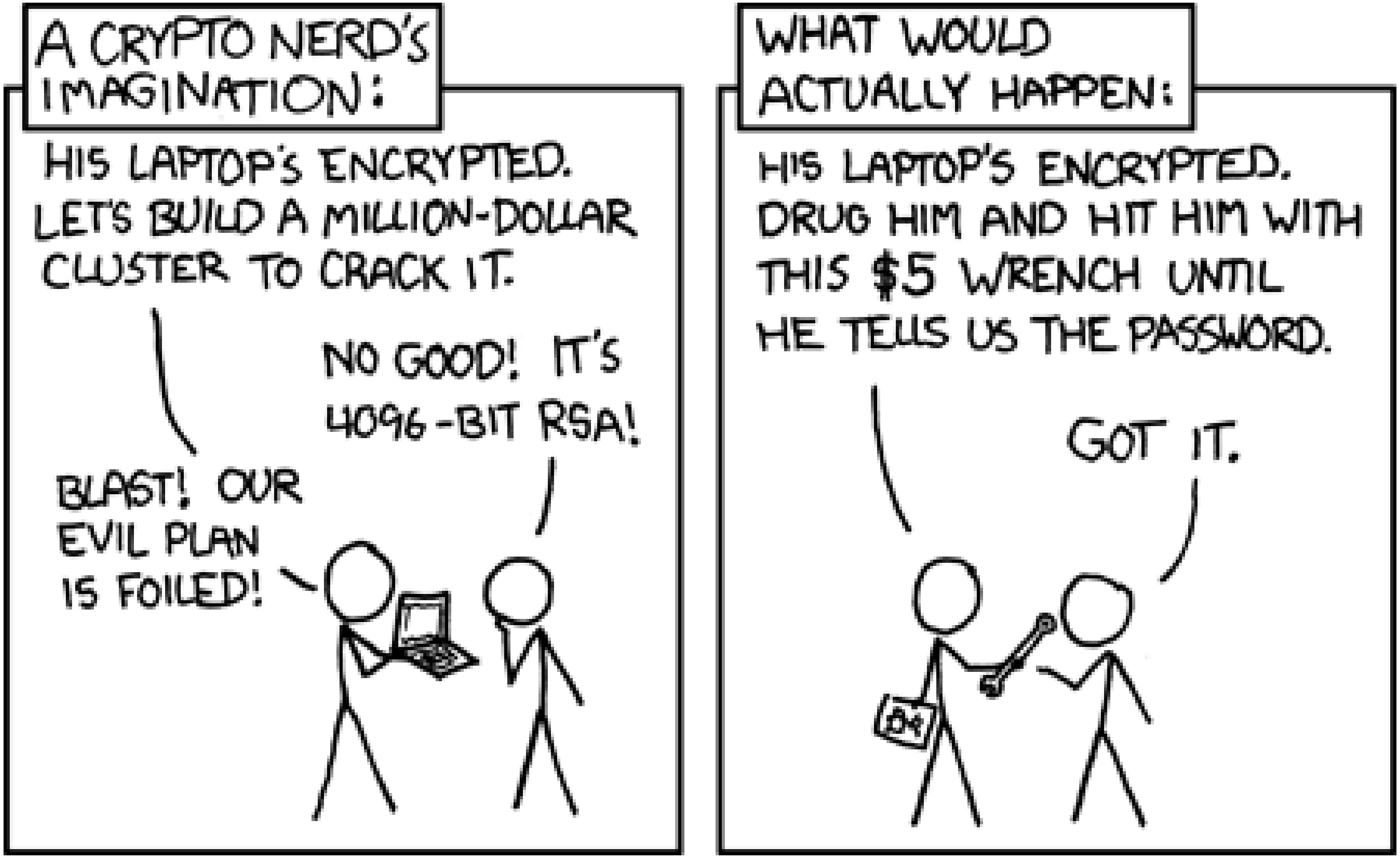
- Use Workspace 2.0 – the data stays in Canada (at UBC)

Impacts



- **Breach notification**
- **Fines of up to $500,000**
- Costs to the Dept
- Reputation damage
- Grants

A Parting Note on Reality vs. What we Think


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

HTTP://XKCD.COM/538/

Information Security Questions?

Contact Larry Carson,

Associate Director, Information Security Management

larry.carson@ubc.ca

604.822.0773

Twitter: @L4rryC4rson