Dr. Richard Reiner
Chief Security & Technology Officer

TELUS Security Solutions

The Security “Profession”

November 2007

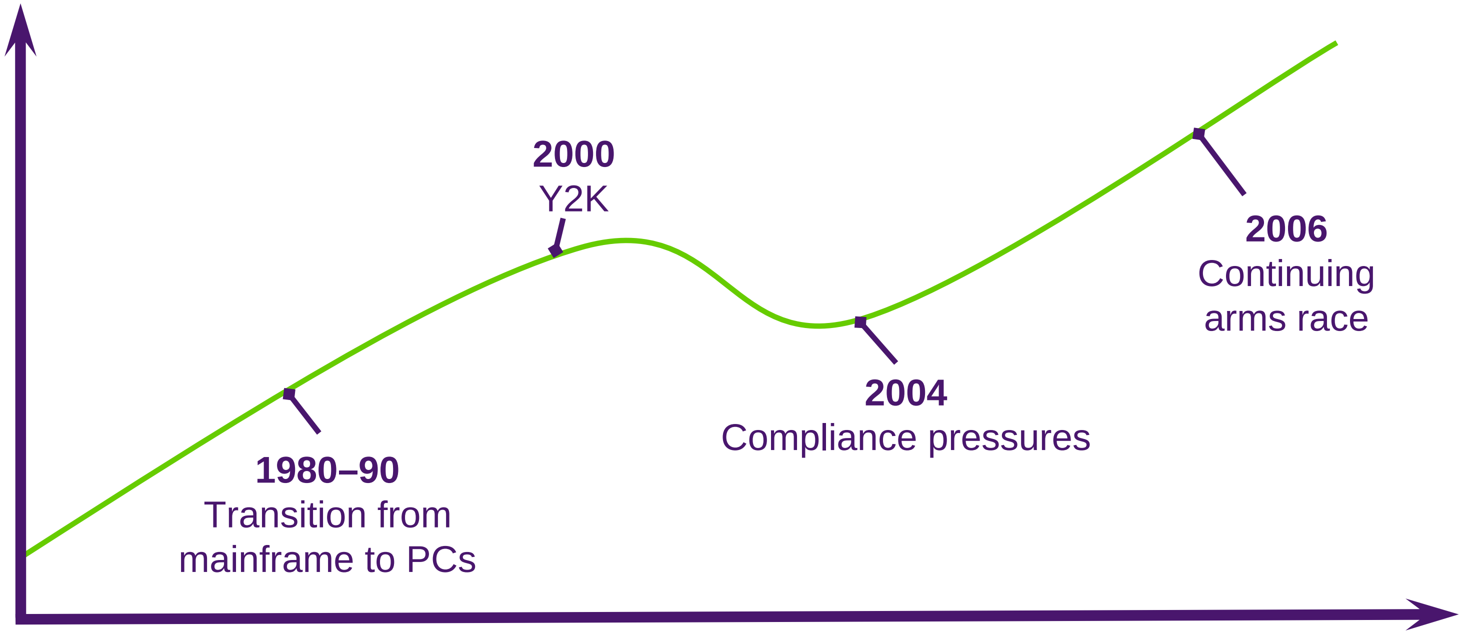
TELUS
the future is friendly®

Questions to consider

- Is information security a profession? Why or why not?
- Do we want it to be?
  - Would it benefit us, as individuals?
- Does the public want it to be?
  - Would it benefit our clients or employers, as organizations?
  - Would it benefit the public?
- What roles or specializations within infosec might be professionalized?
- What would the effects of this be?

Where we are today – Spiralling costs

2007 spending range: from 3% to 10+% of IT budget
(The usual comparison to the IT budget is itself a concern)



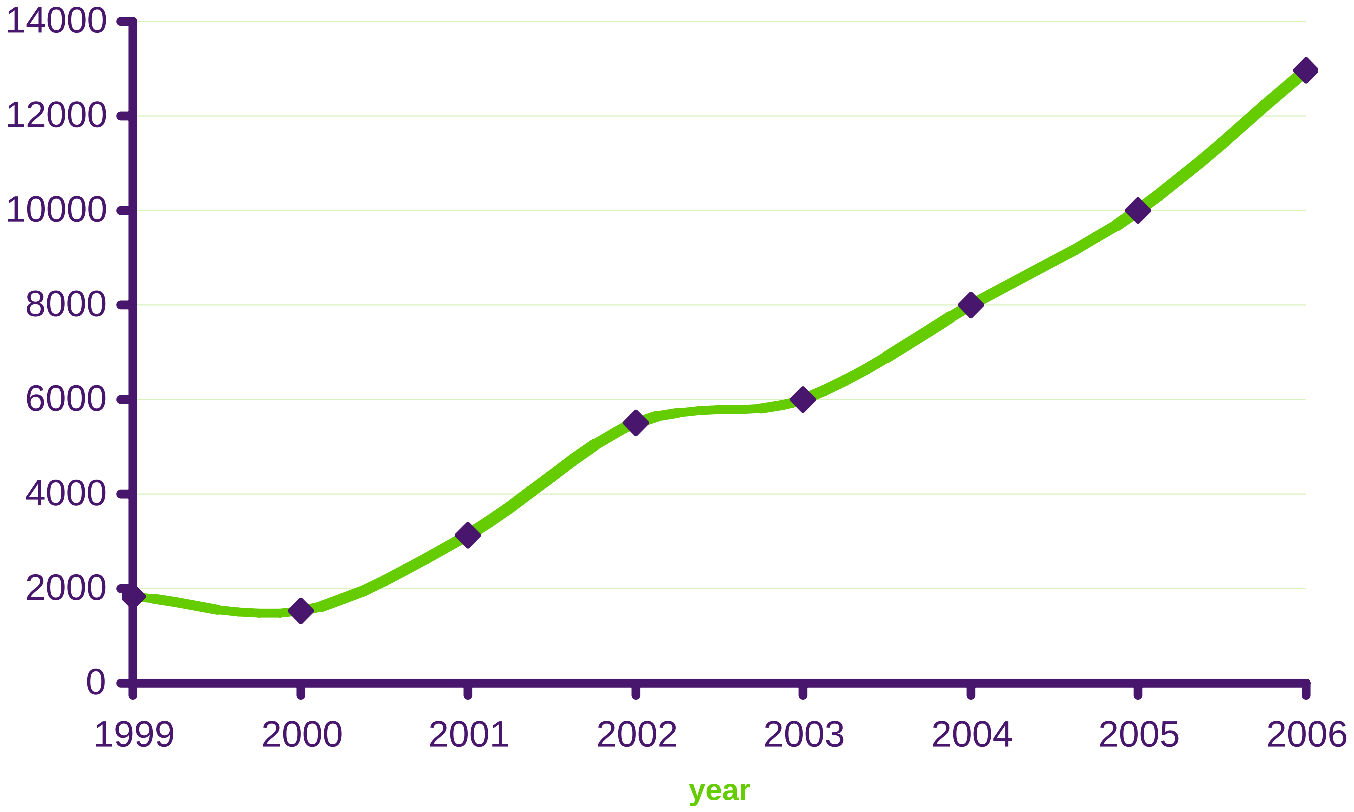
Where we are today – Spiralling costs

CATEGORY	DESCRIPTION	COMPANY A: LOW-PROFILE BREACH IN A NON-REGULATED INDUSTRY	COMPANY B: LOW-PROFILE BREACH IN A REGULATED INDUSTRY	COMPANY C: HIGH-PROFILE BREACH IN A HIGHLY REGULATED INDUSTRY
discovery, notification & response	Outside legal counsel, mail notification, calls, call centre, and discounted product offers	$50	$50	$50
lost employee productivity	Employees diverted from tasks	$20	$25	$30
opportunity cost	Customer churn and difficulty getting new customers	$20	$50	$100
regulatory fines	FTC, PCI, SOX	$0	$25	$60
restitution	Civil courts may ask to put this money aside in case breaches are discovered	$0	$0	$30
additional security & audit requirements	The security audit requirements levied as a result of the breach	$0	$5	$10
other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	$0	$0	$25
Total cost per record		**$90**	**$155**	**$305**

Source: Forrester Research Inc., 2007

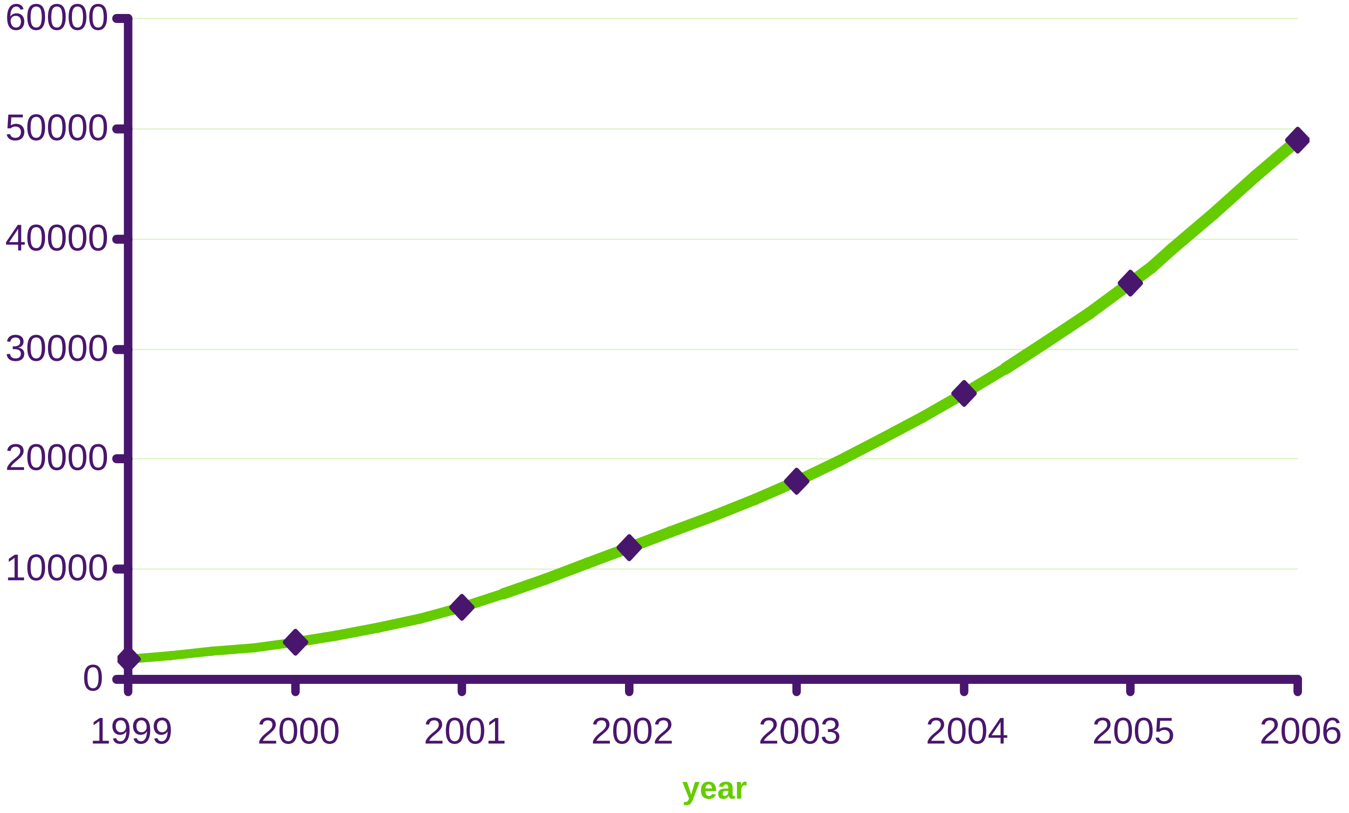
Where we are today – a flood of new entrants

CISSP certifications issued per year



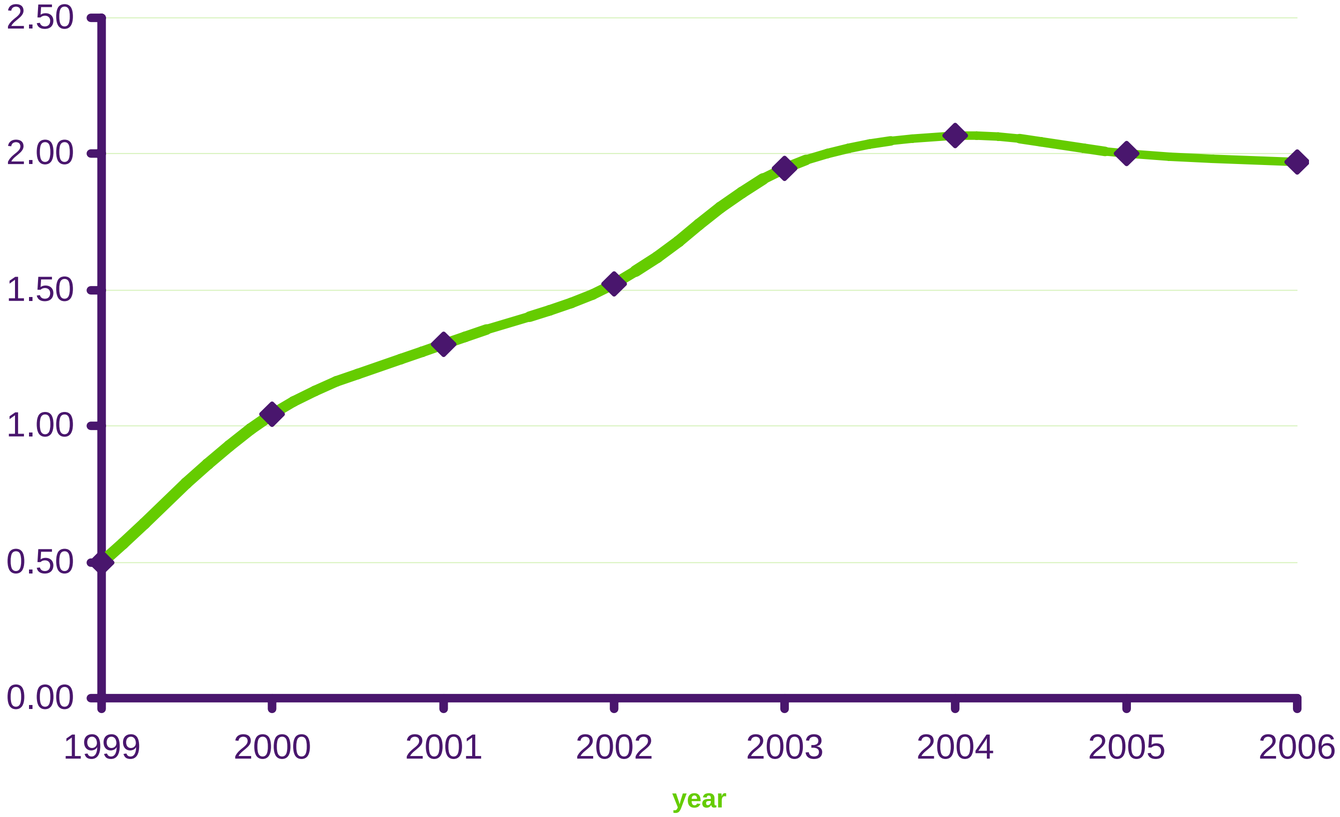
Where we are today – a flood of new entrants

Cumulative number of certified CISSPs



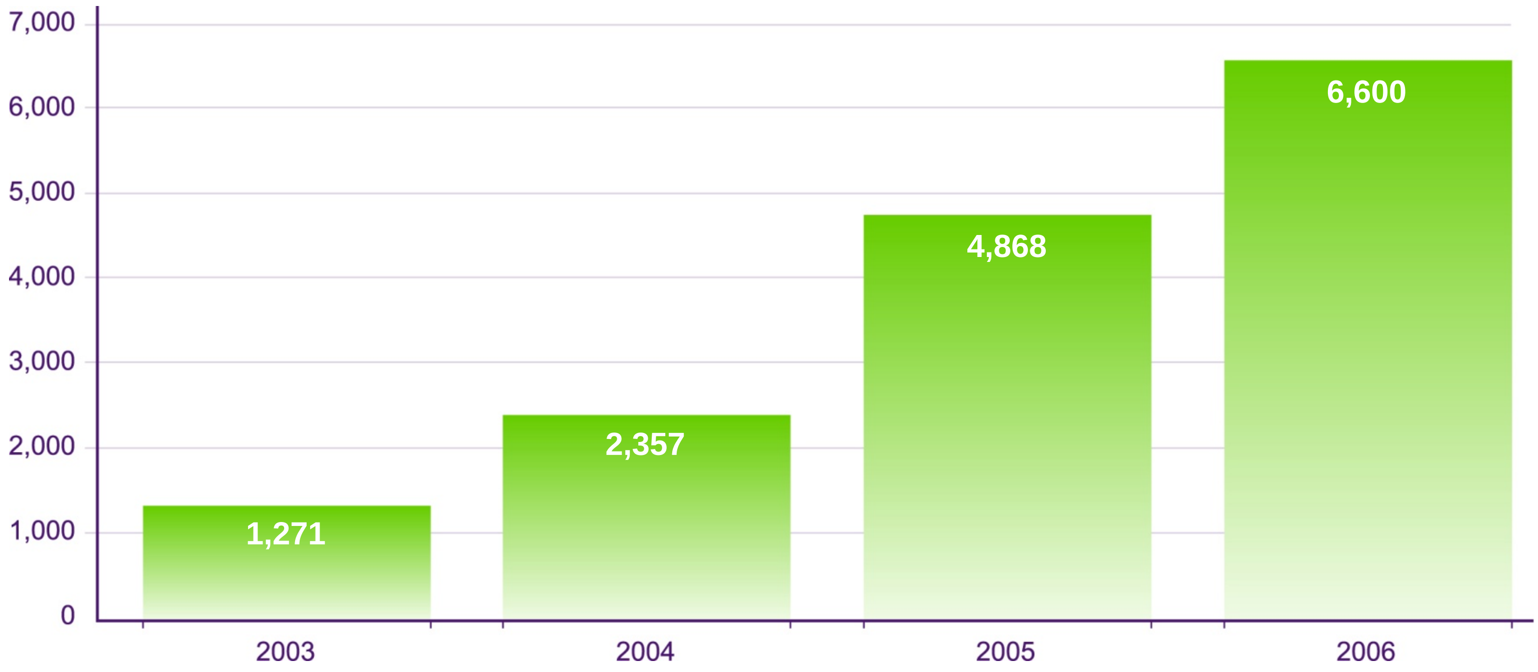
Where we are today – declining mean skill level

Average years of CISSP experience



Where we are today – increasing risks

Security faults in software & networking products



Where we are today – organizational capabilities

Our information security capabilities are still in a primitive state

- Complex technology, regulatory, and economic environment has created a tremendous challenge
- In the early 20th century, businesses had Chief Electricity Officers
  - Electricity was new, complex, challenging
  - Electricity presented new opportunities, and new risks
- Today we have Chief Information Security Officers
  - New information flows are complex, challenging, and present new opportunities
    as well as new risks
- The creation of specialized roles like these is a rational response to an urgent challenge
  - But we don’t have Chief Electricity Officers any more

Where we are today – a stronger adversary

“Professionalization” of cybercrime

- Hacking has transformed from a hobby to a criminal business over the last 18-24 months
- Involvement of organized crime
  - Emergence of cyber-extortion: DDoS and crypto-worms
- Criminals are now the main agents of attacks
- Profit motive
  - Corporate espionage (e.g. spear phishing)
  - Escalating identity thefts

Are we meeting the challenge?

- We have a problem, Houston
  - Inadequate response to growing threats

- One solution that has been suggested: “professionalize” the security industry

What is a professional?

- There is a recent, loose sense of the term:
  - “Professional gambler”
  - “Professional clown”
  - “Professional fry-cook”
  - “Professional cat-burglar”
  - “Professional psychic”

- In this sense, a “professional” is someone who does anything at all, on a full-time basis, generally for money
  - We’re all professionals!
  - Nothing much to debate here
  - But is there more to this?

What is a professional? (2)

- There is a more substantial meaning:

  “Engaged in one of the learned professions … characterized by or conforming to the technical or ethical standards of a profession”

  (Merriam-Webster)

- A professional is a member of a *learned group*, possessing its own *technical standards* and/or *ethical standards*

➔ “The self-regulating professions”

Self-regulating professions

1. A profession renders a unique, definite and essential service to society – only members of the profession render the service and the service must be considered so important that it is available to all members of society. For example, only lawyers practice law, medical doctors practice medicine, and accountants practice accounting
2. Relies on intellectual skills in the performance of its service
3. Has a long period of specialized training
4. Both individual members of the profession and the professional group enjoy a considerable degree of autonomy and decision-making authority. Professional groups regulate their activities rather than having outsiders set policies and enforce adherence to standards
5. A profession requires its members to accept personal responsibility for their actions and decisions
6. A profession emphasizes the services rendered by its members rather than their financial rewards
7. A profession is self-governing and responsible for policing its ranks
8. A profession has a code of ethics that sets out the acceptable standards of conduct for its members

(Ryan and Cooper, 1988)

How does a self-regulating profession operate?

1. Governments possess the exclusive (usually constitutional) right to regulate work
   - Usually a constitutional right
   - Sometimes a right of national governments; in US and Canada state / provincial respectively
2. Recognition of a profession by legislation
   - E.g. “Medical Practitioners Act”, “Legal Profession Act”
   - About 20 professions recognized in most jurisdictions… doctors, dentists and lawyers, but also architects, surveyors and foresters
3. Delegation of regulatory power by the government to bodies representing the recognized profession
   - Generally two bodies: one charged to protect the interests of the members of the profession, the other charged to act in the interest of the public

How does a self-regulating profession operate?

4. Boards are composed of members of the profession (elected by the profession) plus members of the public (appointed by the government)
   - Inclusion of members of the public is meant to balance interests of the members of the profession and public interests
5. Boards responsible for:
   - Admission to the profession – licensing
   - Accreditation of educational programs
   - Quality assurance – periodic testing
   - Continuing education
   - Enforcement of codes of ethical conduct – disciplinary processes
   - Actioning complaints from the public
6. Decisions of the Board are subject to review and reversal by the courts

Why self-regulating professions?

- Government can’t effectively regulate specialized fields
  - Difficulty of regulating a specialized field without specialized theoretical knowledge
  - Difficulty of regulating a specialized field without experience in the field
- Need to balance interests of members of the profession…
  - High fees!
  - Short hours!
  - No personal risk!

… with those of the public

  - Low costs!
  - Easy access!
  - Maximum accountability!

Alternatives to self-regulating professions

- No regulation
  - Clowns, gamblers, cat-burglars
- Voluntary or discretionary credentials
  - No exclusionary rights – anyone can practice
  - This is where we are today!
    - Exception: audit
  - CISSP, GIAC, etc.
- Direct government regulation
  - E.g. lawyers in most civil law (vs. common law) jurisdictions
    - Responsible directly to the Ministry or Department of Justice in the Executive Branch of government
    - Primary responsibility is to the State (vs. the profession or the public)

The information security “profession” today

- No full-blown self-regulating profession in infosec is currently recognized, anywhere (AFAIK)
  - Exception: IT Audit, which is controlled by the self-regulating profession of accountancy

- Few jurisdictions have direct government regulation of (commercial) infosec
  - Some exceptions, e.g. South Korea

- To a great extent, we’re in with the clowns and the cat-burglars

Do we want to change this?

- Benefits to individual practitioners
  - Reputation / status – through keeping better company (exclusion of unqualified practitioners)
  - Organized support for financial interests of practitioners
  - Improved quality of educational opportunities

- Obligations for individual practitioners
  - Formal, demanding admission criteria
  - Continuing education obligations
  - Obligation to act in the public interest
  - Obligation to adhere to a uniform ethical code (not a personal one!)
  - Complaints process, with disciplinary consequences
  - Strong potential for adversarial relations between practitioners and the governing body

Do we want to change this? (2)

- Benefits to the public
  - Reliable access to quality practitioners with up-to-date knowledge
  - Assurance that practitioners will act in the public interest
  - Assurance that practitioners will adhere to a uniform ethical code
  - Access to a complaints process, with disciplinary consequences

- Obligations for the public
  - Recognition of status
  - Appropriate compensation structures

Who might be included?

- Enterprise (defensive) practitioners
  - Obvious candidates for inclusion – in the public interest
- Offensive practitioners (Intelligence, Military, Law Enforcement)
  - Less clear-cut case… but public-interest argument applies
- Product development people
  - Product quality
  - Malicious functionality: backdoors, etc.
- Researchers? Nah!
  - Well, maybe…
  - Research in other fields is often included (e.g. medical)
  - Responsible disclosure, experimental ethics, etc.

Summary

- Creation of a self-regulated infosec profession would appear to be in the public interest

- Less clear that it is wholly in the narrow self-interest of practitioners
  - Just ask MDs how they feel about their professional Colleges!

- Are we prepared to put the the public interest ahead of risks to narrow self-interest?

TELUS Security Solutions

Questions & Comments

TELUS

the future is friendly®