The University of Toronto’s Information Security unit priorities, 2019–2020

Identify:
- Creating and implementing a University-wide and department-championed information security risk assessment program.
- Documenting security standards baselines.
- Creating a new data classification model.
- Facilitating the growth of information security awareness and training.

Protect:
- Continual monitoring and improvement of Office 365 security.
- Maintaining a strong gateway firewall.
- Continuing the expansion of U of T's multi-factor authentication features and protocols.
- Further developing the University’s VPN service.

Detect:
- Maturing the University’s vulnerability management program.
- Advancing U of T’s security event monitoring system.

Respond:
- Creating and finalizing incident response playbooks.
- Establishing retainers with incident response service provider(s).

Recover:
- Facilitation of table-top exercises.
- Reviewing the University’s existing information back-up strategies.

@ITSUOFT  https://isea.utoronto.ca/
The ‘old’ security model:

• End state: “we are secure”.
• Information security is IT’s job.
• Lock it down.
• Plugging the holes.
• A solution in search of a problem.
• Security versus convenience.
• “If only we had more money/time/people.”
• See no evil, hear no evil, speak no evil.

The ‘new’ security model:

• End state: managed risk.
• Information security is everyone’s responsibility.
• Enable the mission and values of the University.
• Empower individuals and units.
• Allocate resources based on risk.
• Assume you are breached. Find the intruders and kick them out!