Good morning, I am pleased to be with you today for the launch of the JCSE Skills Survey. I am Moira de Roche, Chair of IFIP IP3 (International Professional Practice Partnership). IP3 was created by IFIP International Federation for Information Processing (the UNESCO created umbrella body for national ICT bodies) in 2007 to carry out the IFIP strategic goal of ICT as a Global Profession. We work to set and maintain the Professional Standards, and accredit member bodies against these standards.

To focus on partnership, and emphasising the important of Trust – which I will speak about today - our new tag line is "Partnering for Trust in Digital. "

Before we consider the why Trust is so important, let's contemplate what makes a professional:

- Skills and Knowledge, with demonstrated competence, along with continuous professional development, which is essential in any profession, but even more so in ICT where things change so quickly
- A service mind-set for internal and external customers, and the community at large
- Trustworthiness – the Trust I alluded to earlier, and will throughout this address
- Accountability to himself or herself and his or her employers, and for any product created by them
- Ethics – subscribes to and lives by a code of conduct, and always behaves in an ethical manner
- Pride in the profession, with a desire to protect the profession.

I found this on the ACCA global, the body for Accounting professionals, site "Ethical principles and behaviour will become more important in the evolving digital age, and a key enabler to building trust". IP3 are not alone.

Trust can be defined as a firm belief in the reliability, truth or ability of someone or something. Synonyms include: confidence, certainty, assurance, reliance.

Until not very long ago, we thought – if we thought about it at all – that some natural disaster or apocalyptic event would herald the end of the world. The Four Horsemen of the Apocalypse, and the predictions of Nostradamus come to mind.

Today, we have an almost total reliance on technology, so perhaps it's more likely that technology rather than nature or the wrath of God will cause a catastrophic end.

Suppliers and users can be anywhere. We don't know who we are dealing with – we don't even know if we are dealing with humans.

If you are anything like me, you have an "there's an app for that" mentality. I am an app junkie, I just can't get enough…… But how often do we consider the integrity of the apps we use? Where do they come from, who developed them? Do they care about you and me?

Vulnerabilities and attacks are usually due to unforeseen circumstances. The adverse effects compound exponentially. Whilst we hail the Fourth Industrial Revolution as a great step forward, with the Internet of Things - the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors**,**
as a remarkable stride into making our lives easier, we also live with the danger of malicious software in that same internetworked cyber-physical system. I am reminded of a delegate at WSIS earlier this year who mentioned a baby monitor, linked to other devices, that came with a pre-set password that she was unable to change. This made her very uncomfortable, but the reality is that most of us simply take it for granted.

Why is trust an issue? Confidence in the use of tech will limit or enable economic growth. Retreating into a safe place and not using the power of tech is not an option. We must improve trust in technology, and amongst humans, bearing in mind that Trust is a multidisciplinary concept that includes: Security; Safety; Reliability; Usability

Trust is eroded with each attack or malfunction. Consumers are unable to evaluate the security of service providers. They have no way of knowing if security is built in at every level of a product. Apart from the initial creation of a product, maintenance and usability of the product should be part of the security "value-chain".

Security and Privacy competence and knowledge is an essential digital skill in the 21st Century. It is necessary for technologists and end-users alike. All of us are at risk - talk to colleagues about this: almost everyone has a embarrassing but scary story to tell.

If we use Credit Cards on an e-commerce site, how safe are these details. In September, the world was shocked by the Equifax hack. For those of you who are not familiar with them, Equifax do credit checks for credit card applicants. You would probably expect an organisation like this to be extra vigilant – I sure would – but the organisation fixed a known bug on the Apache software used on the web server three months late.

The Wannacry ransomware that wreaked havoc in the last year emanated from a government hacker toolkit! The NHS was a victim, because they use Windows XP. Now, I realise there is a huge cost to upgrading to new versions of operating systems but surely this would have been a wise investment. It serves as an example of the criticality of IT. When we first embarked on creating a global ICT profession, we often heard "But ICT is not life-threatening". There were patients on NHS whose operations had to be delayed – that was potentially life-threatening. Others who came for emergency care which could have been compromised because the care givers could not access their health records. I don't think anyone was intentionally negligent, probably just unaware of the potential for harm.

TechRepublic reports that Ransomware continues to dominate the Cyber-security landscape in 2017, with businesses large and small paying millions of dollars to unlock encrypted files. The attacks appeared in 64% of all malicious emails sent in Q3, with major successful campaigns such as Notpetya and wannacry showing no signs of slowing down. How do we get people to stop trusting email?

It's also worth remembering that your mobile phone tracks your every move.

We must stop to consider the impact of Artificial Intelligence and Robotics. We can't have this discussion without looking at the Tesla incident, where an "over reliance" on Tesla's driverless technology played a major role in a fatal accident in the US, an independent investigative body has found.
In May last year, a Tesla Model S sedan operating in Autopilot mode – a semi-autonomous driving feature that handles most of the steering and speed on freeways – crashed into a truck that had turned in front of it without giving way, killing the car's 40-year-old driver, Joshua Brown.The National Transportation Safety Board (NTSB) found that the Tesla Autopilot feature had to bear some of the blame for the accident because it had allowed the driver to become over-reliant on it and not pay proper attention to the road.
"The combined effects of human error and the lack of sufficient systems controls resulted in a fatal collision that should not have happened. " Over-reliance on auto pilot meant that the driver trusted auto-pilot to take care of all eventualities. Tesla trusted the driver to still be in control. Both were mistaken and bear the blame collectively. The driver paid the price.

Forbes predict that AI technologies have the potential to increase productivity by more than 40% by 2035. AI will accelerate growth, and is very likely to create new

knowledge and service industries. Experts remind us that AI will augment, not replace, human intelligence. An example of AI for Good, and to improve trust, is to use it to monitor network traffic, flag suspicious behavior or network anomalies, and alert the security team to evaluate.

In response to all of this , IP3 launched iDOCED, the IFIP Duty of Care for Everything Digital Initiative. iDOCED is designed to remind and support both providers and consumers of digital products and services that they have a duty of care in ensuring that they act responsibly in relation to the digital world.

The iDOCED was developed in response to repeated instances of poor ethical behavior by companies. These include low quality, underperforming products, or lack of care by digital consumers.

“We’ve recently seen high profile failures including Volkswagen, who was caught in 2015 using technology to cheat fuel emissions testing, which has cost them nearly US$15 billion in the US market alone,” commented Brenda Aynsley, then chair of IFIP IP3. “On top of that, we’ve seen users compromised by the way they accessed the Internet or used software or various online tools, such as people whose webcams were hacked and used to invade their privacy or even film them without their knowledge.

“The iDOCED seeks to raise awareness of what users can and should do to protect themselves in today’s digitally-connected world, and to highlight the need for companies to act responsibly and ethically in the development and implementation of commercial products and services.”

We can’t stop using technology. The benefits are vast. But we have a duty of care to keep ourselves and other safe. We should demand that our service providers use certified ICT professionals who have demonstrated skills and knowledge.

We can, I believe, expect our governments to understand the contribution of ICT to the economy, and the risk to the economy when things go wrong.

We know that probably most data breaches are not reported, or we are made aware of them when the damage has already been done. Governments must legislate for data breach reporting to assist consumers

We also need government and international organisations to develop defensive and offensive instruments in cyber-attacks. Industry collectives must co-operate in the public interest.

We all have a Duty of Care in the Digital World. We take reasonable care to keep ourselves and our families, and our possessions , safe in the physical world. We only call on law enforcement when things go wrong. We must adopt the same attitude in the Digital World. Cost is not the most important factor – reliability, accountability and the ethics of the creators, developers and providers are.

Those of us in the know, ICT Professionals, have a duty of care to ensure all those around them and they themselves, understand Security and privacy.
We must be aware and vigilant and ask questions about the tools we use. Keep informed, make demands of the legislators. Demand properly qualified and credentialed providers.

IFIP IP3 have a recipe of Trust,
Ingredients

- Competence
- Ethics
- Continuous professional development
- Cyber-Security specialism

Method

1. Exercise proper judgement
2. Choose your provider carefully
3. Ensure privacy & security
4. Value professionalism
5. Demand action from leaders

This dish will last forever, provided you don't skimp on the Ethics.

Thanks