ServiceTec
AirportCyberSec

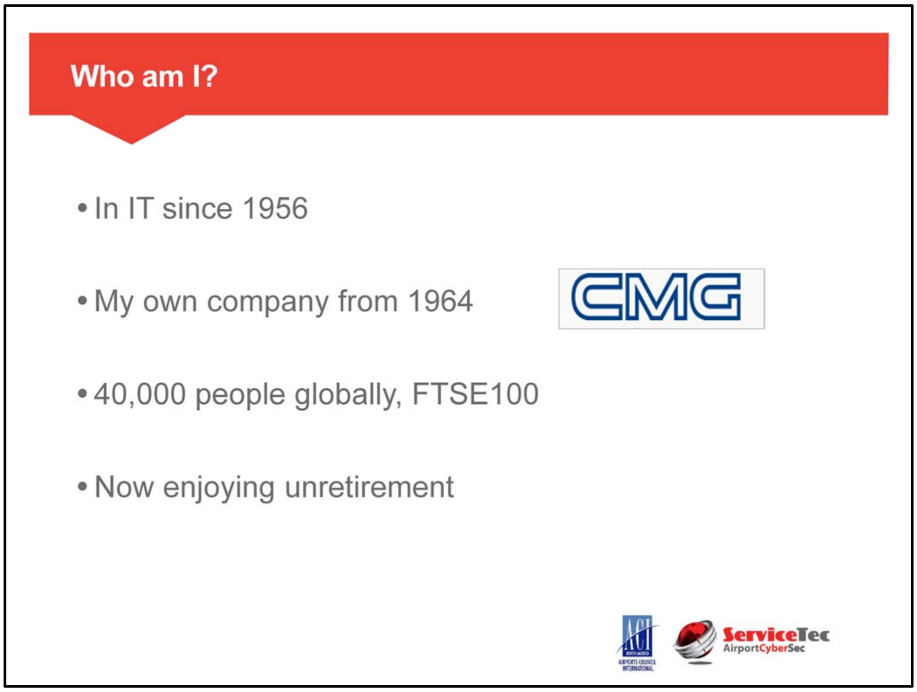
ACI
NORTH AMERICA
AIRPORTS COUNCIL INTERNATIONAL

CyberSecurity – Managing the Human Element

Dr Bryan Mills
Director CyberSecurity,

ServiceTec Airport Services International Ltd

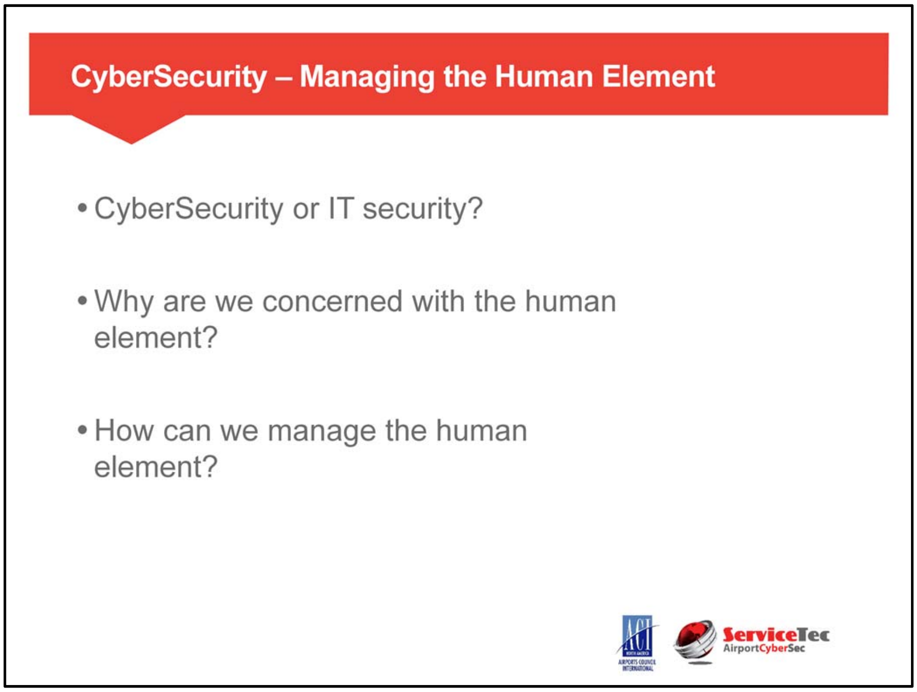
We **safeguard** your **reputation** and **protect** your **revenue**
World class cyber defense for IT systems at airports



Who am I?

- In IT since 1956
- My own company from 1964
- 40,000 people globally, FTSE100
- Now enjoying unretirement

I have been in IT since 1956, and in that time, I have seen the cycles recur as they do in everything – Cyber attacks are the first genuinely new things I have seen. Criminal, malicious and political motivations have always existed – but our newly networked world provides a truly new methodology for their expression

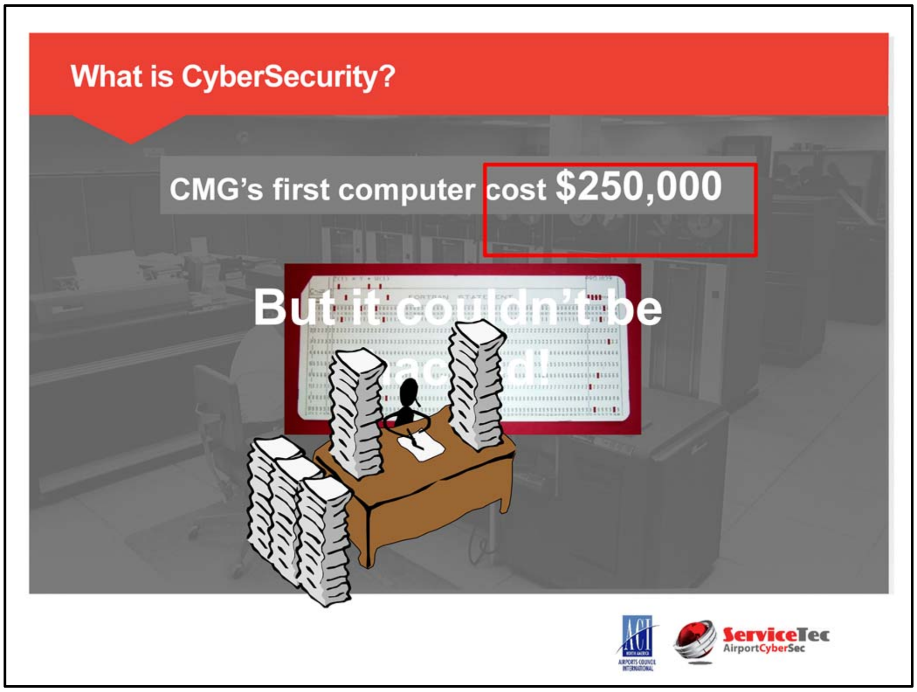


CyberSecurity – Managing the Human Element

- CyberSecurity or IT security?
- Why are we concerned with the human element?
- How can we manage the human element?

Subdivisions of the presentation; I am approaching the topic under three headings

Cyber Security or IT security? Is there a difference?
Why are we concerned with the human element?
How can we manage the human element?

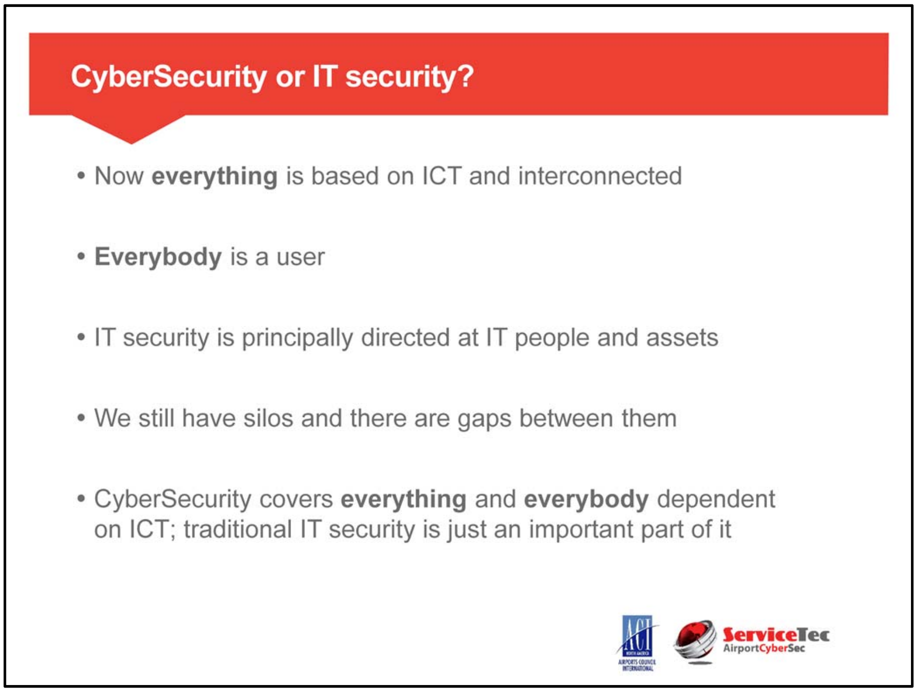


What is CyberSecurity?

CMG's first computer cost $250,000

But it couldn't be hacked!

When CMG bought its first computer, it filled a room and cost $250,000 (1967 money). Its only data input was in the form of punched cards; its memory was 32 **KB;** data storage was in the form of magnetic tape; and its only humanly usable output was printed paper.
BUT it did have one great advantage – it was unhackable, except by somebody who got physical access to the computer room, because it was not connected to anything else.



CyberSecurity or IT security?

- Now **everything** is based on ICT and interconnected
- **Everybody** is a user
- IT security is principally directed at IT people and assets
- We still have silos and there are gaps between them
- CyberSecurity covers **everything** and **everybody** dependent on ICT; traditional IT security is just an important part of it

ServiceTec AirportCyberSec

Cyber Security or IT security?

Is CyberSecurity just a fashionable term for IT security. I believe not, but that there is a significant difference between the two terms because of the environment we now live and work in. In 1967 it was not the case that:-

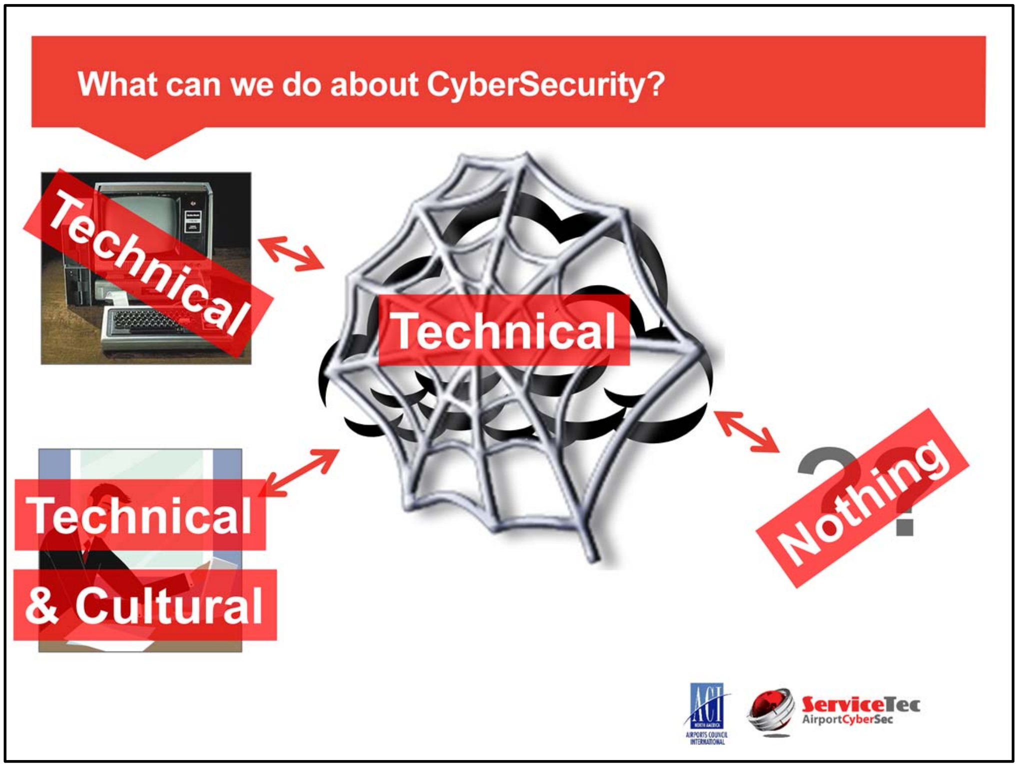
everything is based on ICT and interconnected. (or nearly everything, and more and more all the time)

Everybody is a user.

IT security is principally directed at IT people and assets, and historically this has been the right thing and it still remains the fundamental thing.

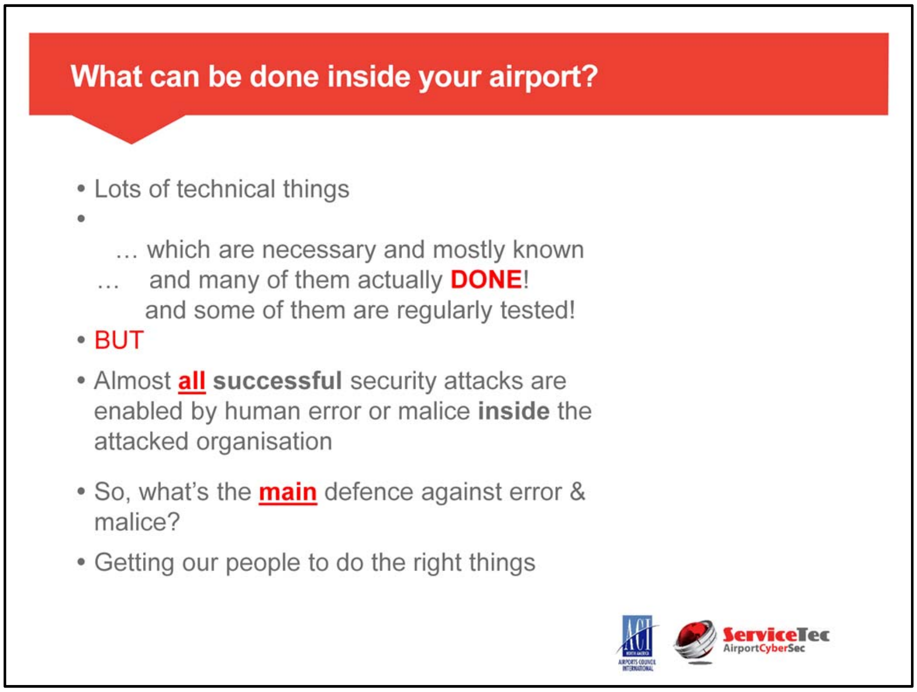
We still have organisational silos and there are gaps between them; these silos often have their own IT activities and all their staff are connected, but the gaps provideways for attackers to break in.

Cybersecurity covers **everything** and **everybody** dependent on ICT; traditional IT security is a most important part of it, but only a part.



What can we do about CyberSecurity?

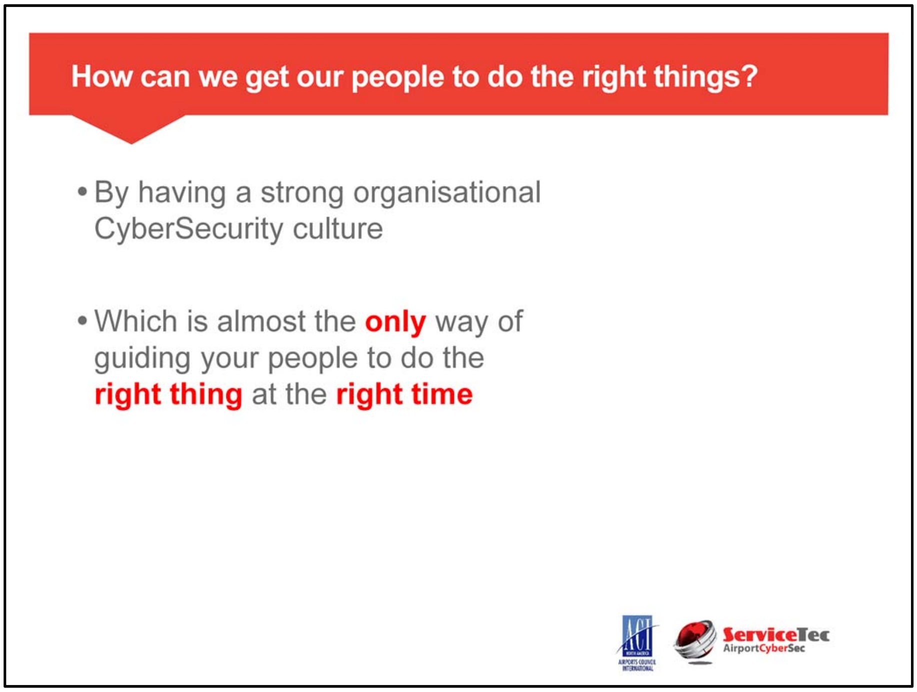
What can be done inside your airport?
First of all, obviously, technical best practice has to be implemented and then regularly checked; your technicians are only human; your network is very complicated; the attackers are many and smart. You have to defend against many attackers – only one of them has to get through. You cannot act upon the world to which your people and assets are connected to via the internet; your defences have got to be focussed, in depth, on what you do control, and in the case of the people using your network, that control has to be technical and cultural.



What can be done inside your airport?

- Lots of technical things
-

  … which are necessary and mostly known
  … and many of them actually **DONE**!
  and some of them are regularly tested!
- BUT
- Almost **all** **successful** security attacks are enabled by human error or malice **inside** the attacked organisation
- So, what's the **main** defence against error & malice?
- Getting our people to do the right things

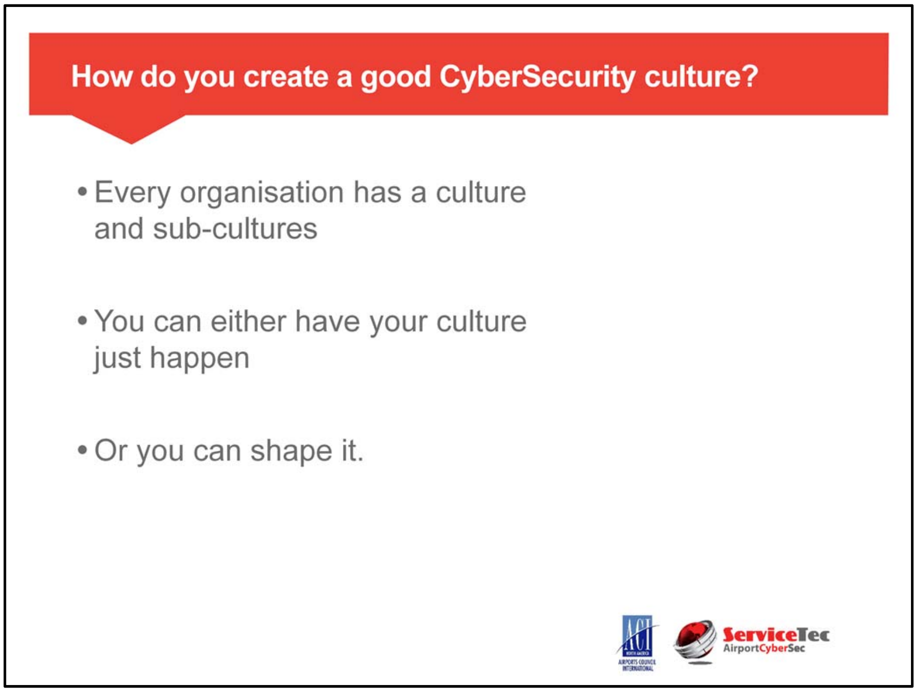


How can we get our people to do the right things?

- By having a strong organisational CyberSecurity culture
- Which is almost the **only** way of guiding your people to do the **right thing** at the **right time**

ServiceTec
AirportCyberSec

How can we get our people to do the right things?
By having a strong organisational cybersecurity culture which is almost the **only** way of guiding your people to do the **right** thing at the **right** time. Airports are service businesses; service can only be delivered by people, and you cannot micro-manage those people's behaviour at the critical moments. In the same way, you cannot truly micro-manage people's behaviour as users of your IT and other assets. Most people want to do the right thing, but they need to know what that right thing is – helping them to know that is what an organisation's culture does.

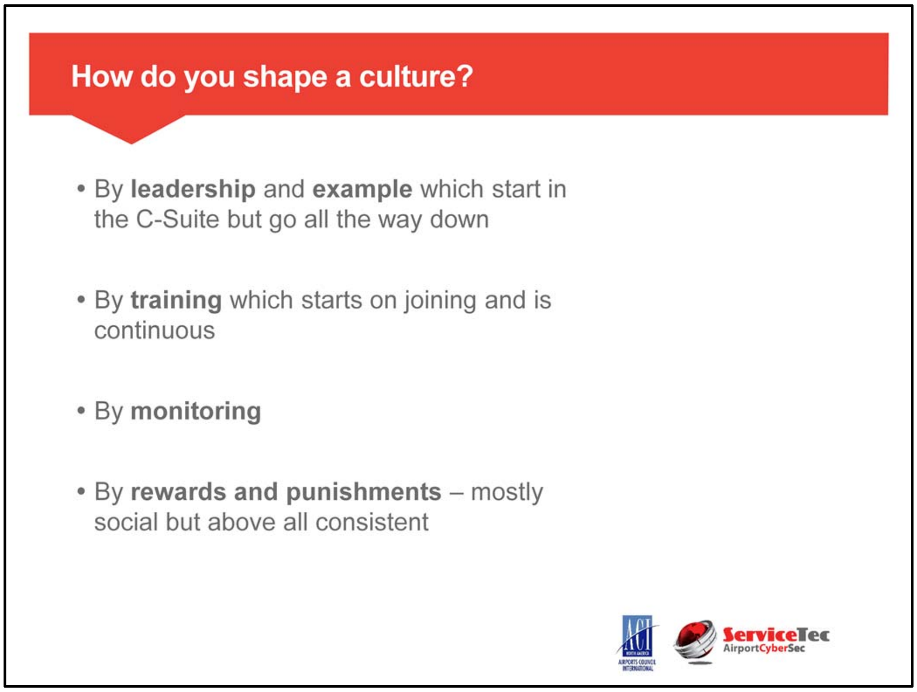


How do you create a good CyberSecurity culture?

- Every organisation has a culture and sub-cultures
- You can either have your culture just happen
- Or you can shape it.

ACI
AIRPORTS COUNCIL INTERNATIONAL
ServiceTec
AirportCyberSec

How do you create a good CyberSecurity culture?
Every organisation has a culture and sub-cultures – you can either have your culture just happen, or you can shape it. If you let it just happen, you cannot be in control of the results.



How do you shape a culture?

- By **leadership** and **example** which start in the C-Suite but go all the way down
- By **training** which starts on joining and is continuous
- By **monitoring**
- By **rewards and punishments** – mostly social but above all consistent

ServiceTec
AirportCyberSec

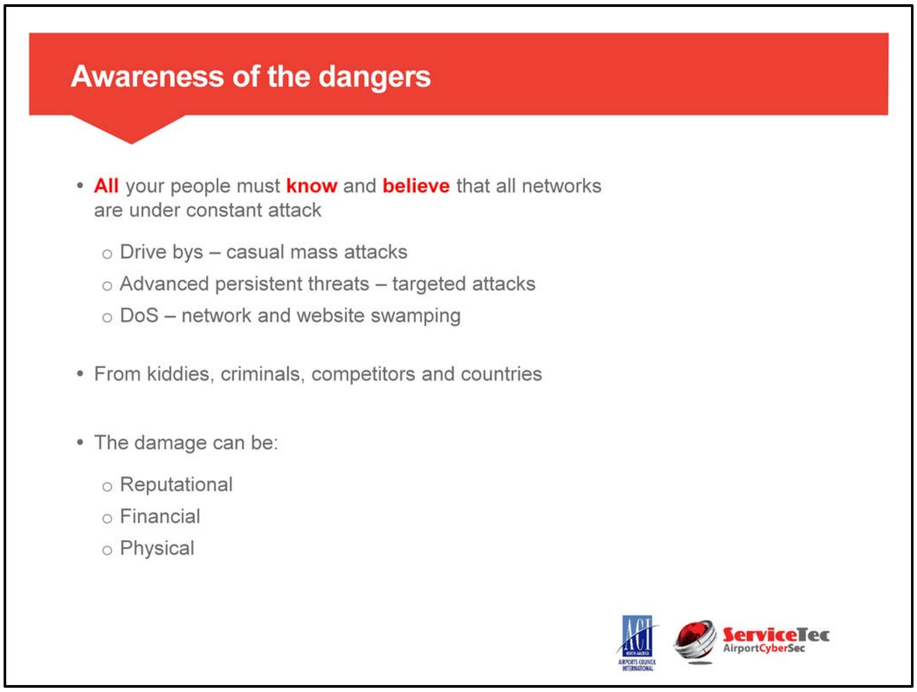
How do you shape a culture?

by **leadership** and **example** which start in the C-Suite but go all the way down. The way in which your airport's culture(s) will be formed is by the leadership and example of the people at the top. People want to respect the leaders – if they can't where does that leave them? So, consciously or unconsciously, people will follow their leaders' examples.

by **training** which starts on joining and is continuous. Training is how you tell people what you expect of them; cybersecurity training needs to start on joining, and be constantly refreshed – the enemy is smart, and manifold, so new forms of attack are constantly being developed.

by **monitoring**; you must know what's happening. This means looking at logs, testing, and probably installing monitoring software, and then taking action on what you discover (see rewards & punishments).

by **rewards and punishments** – mostly social but above all consistent. The rewards are just praise and encouragement; the punishments are "We don't do that sort of thing round here" and eventually formal disciplinary.



Awareness of the dangers

- **All** your people must **know** and **believe** that all networks are under constant attack
  - Drive bys – casual mass attacks
  - Advanced persistent threats – targeted attacks
  - DoS – network and website swamping
- From kiddies, criminals, competitors and countries
- The damage can be:
  - Reputational
  - Financial
  - Physical

ACI
AIRPORTS COUNCIL INTERNATIONAL
ServiceTec
AirportCyberSec

Awareness of the dangers

All your people must **know** and **believe**

That all networks are under constant attack from

Drive bys – casual mass attacks;

Advanced persistent threats – targeted attacks

DoS– network and website swamping

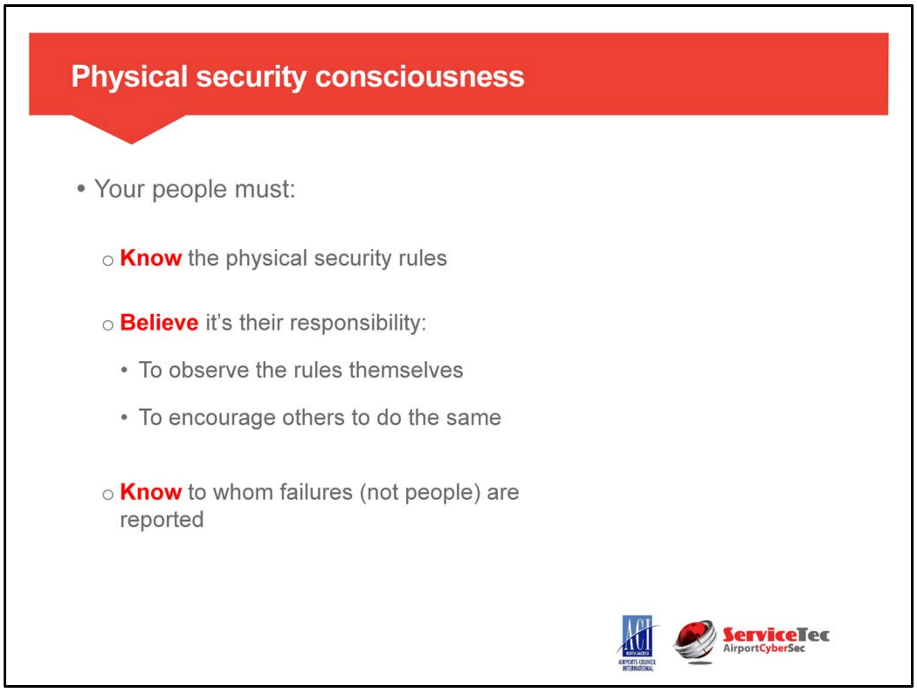
From kiddies, criminals, competitors and countries

The damage can be

Reputational

Financial

Physical



Physical security consciousness

- Your people must:
  - **Know** the physical security rules
  - **Believe** it’s their responsibility:
    - To observe the rules themselves
    - To encourage others to do the same
  - **Know** to whom failures (not people) are reported

ACI
AIRPORTS COUNCIL INTERNATIONAL
ServiceTec
AirportCyberSec

Physical security consciousness

Your people must

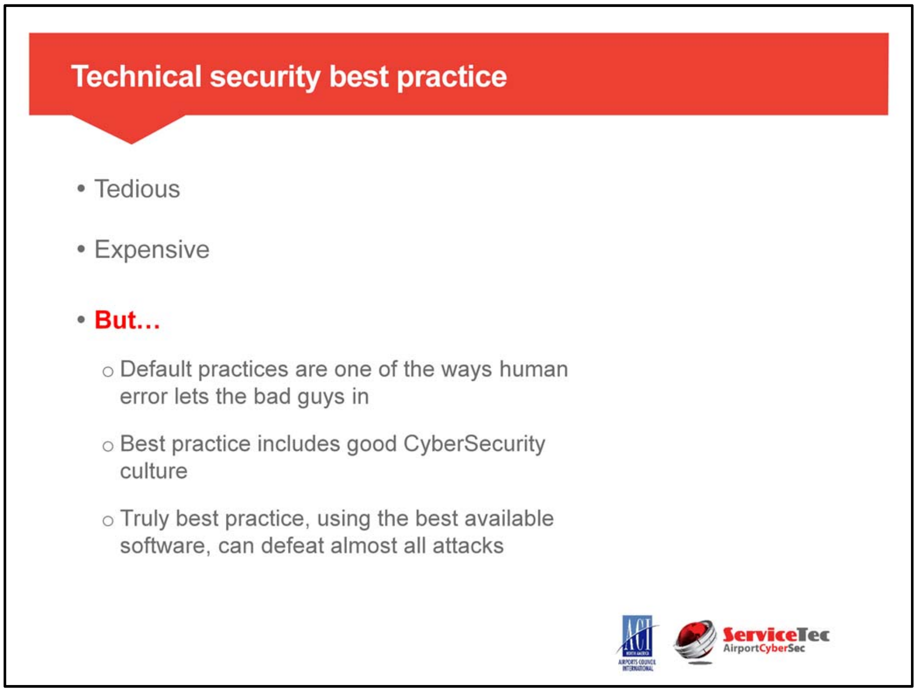
Know the physical security rules

Believe it’s their responsibility

to observe the rules themselves

to encourage others to do the same by commenting on insecure behaviours

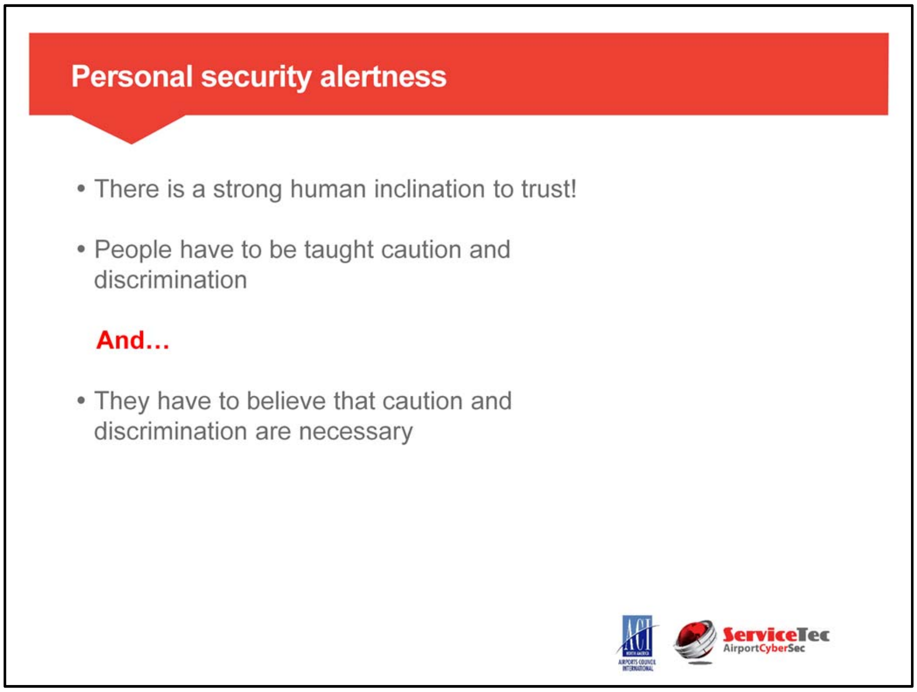
Know to whom failures (not people) are reported; for example making sure that door keypads are functional.



Technical security best practice

- Tedious
- Expensive
- **But…**
  - Default practices are one of the ways human error lets the bad guys in
  - Best practice includes good CyberSecurity culture
  - Truly best practice, using the best available software, can defeat almost all attacks

Technical Security best practice
Networks are as we know immensely complicated; keeping them up to date is tedious and expensive. However default settings, out of date patches are some of the ways the attackers can get in.
Truly best practice has to include the development and maintenance of a good cybersecurity culture, including for your CIT technicians and management.
There is no doubt that best practice and modern defensive and monitoring software can defeat almost all attacks.



Personal security alertness

- There is a strong human inclination to trust!
- People have to be taught caution and discrimination

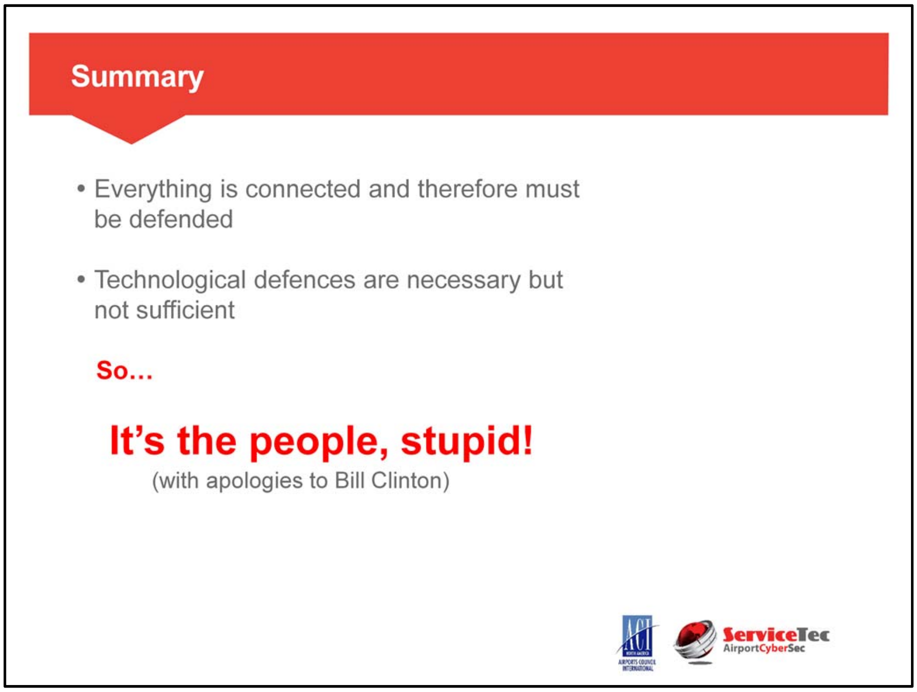
And…

- They have to believe that caution and discrimination are necessary

ServiceTec
AirportCyberSec

Personal security alertness

There is a strong human inclination to trust! Society could not work otherwise. People have to be taught caution and discrimination AND they have to believe that caution and discrimination are necessary. In order to do this, people have to be told how social engineering attacks work, so that they don’t open spear-phishing e-mails; they know what a “waterhole” looks like; USB’s they have found or been given are potentially dangerous (the latest attack form blows up the computer by interfering with the electrical circuits).



Summary

- Everything is connected and therefore must be defended
- Technological defences are necessary but not sufficient

So…

It’s the people, stupid!

(with apologies to Bill Clinton)