

Helping TEC providers navigate the digital transition: a risk-based approach

TSA Special Interest Group 008 - Update June 2020

> Steve Gates MD PPP Taking Care

Why are we even here talking about this: a unique PPP Taking Care perspective?



Consumer/retail-orientation



Technology-agnostic



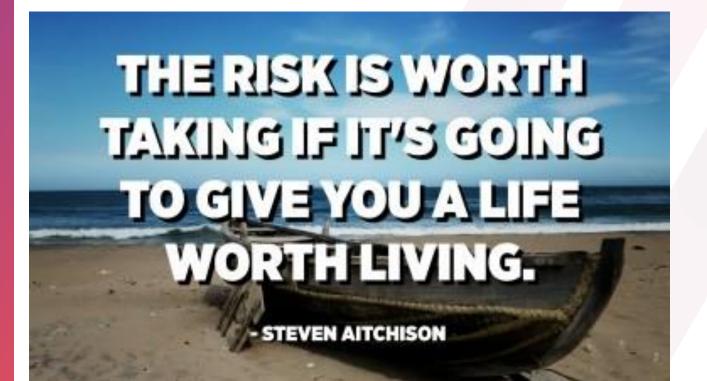


Passionate – TSA SIG sponsors



Owned by AXA

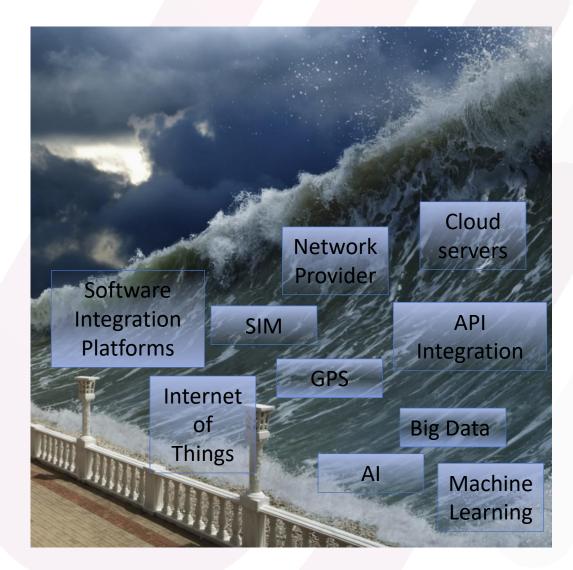
Life is all about risk.....







But we're possibly trying to manage a tidal wave of new risks with old tools/analogue ways of thinking..





Because the 2025 digital switchover is all about risk too...



- I'm not going to think about it...
- A lot can change before 2025...
- When was the last time BT ever delivered anything on time?
- I've got bigger immediate concerns...

BUY NOW!

Click Here To Buy Now

PayPal VISA CONTRACTOR DIS

- Buy our new digital equipment
- Rip out all legacy devices/processes and replace it with new digital kit
- If you don't do this then people will die



Let's not forget – we start from a very resilient standpoint





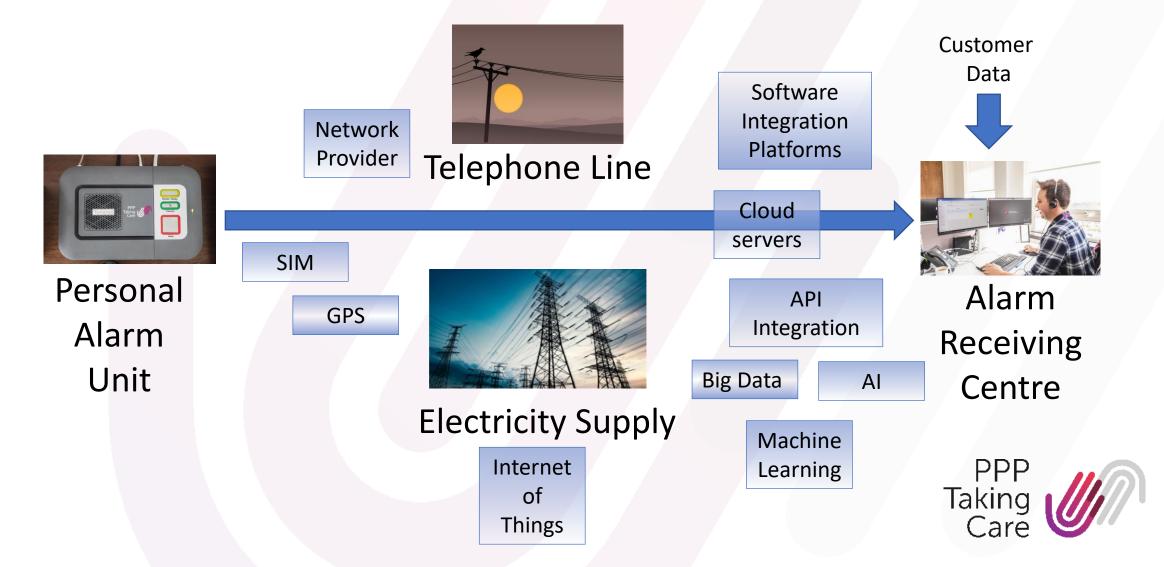
So when we're talking data security, don't forget

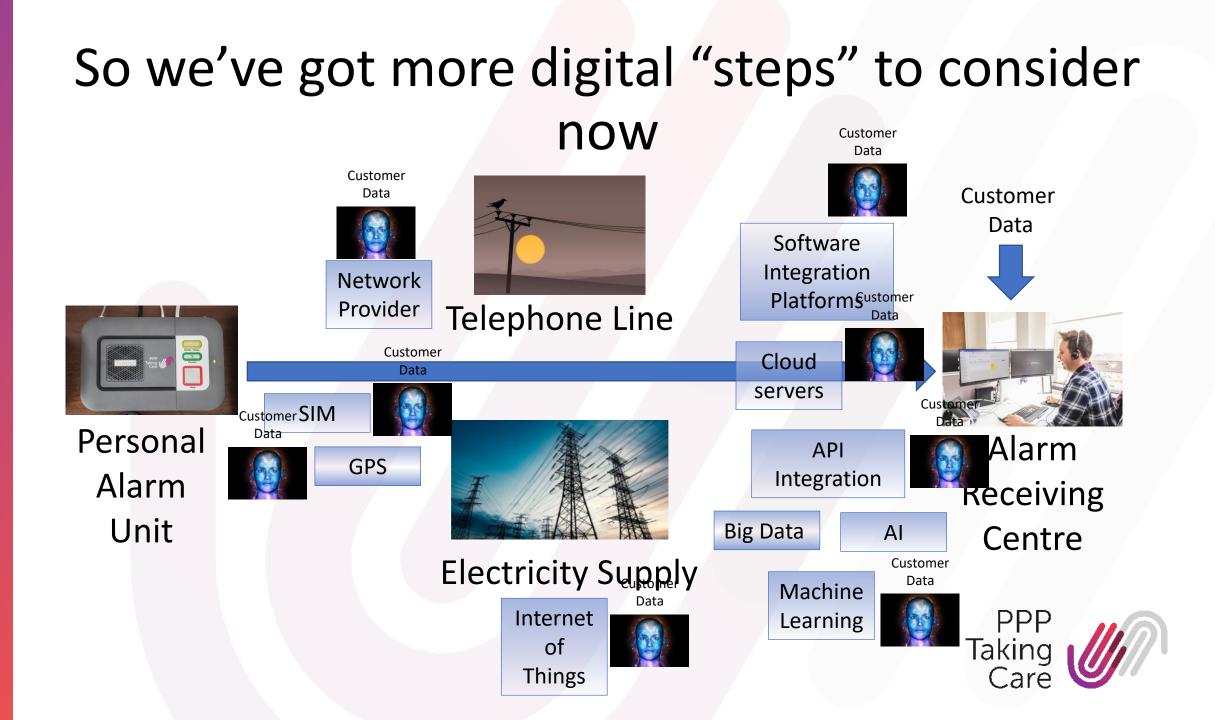


"At the end of the day, no one tries to hack a fax machine..."



So we've got more digital "steps" to consider now





So as a TEC industry we need

To understand how much of the old world will work in the new world

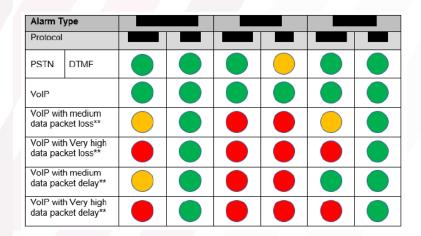
To understand the new standards that will apply in the new world

Communicate clearly about what differentiates us



To understand how much of the old world will work in the new world

- Which devices/platforms are going to work best and for how long using the new digital network?
- We can't simply assume that **nothing** will work.....
- Risk evaluation of your current devices/estate on the new digital network
- What is your weakest "link" deal with that first as the most serious risk?
- TSA can potentially provide a united front/standard for device testing?





To understand the new standards that will apply in the new world



Overall guide

The bigger picture of where the standards fit in

2018

Information and technology for better health and care

Copyright © 2017 Health and Social Care Information Centre. The Health and Social Care Information Centre is a non-departmental body created by statute, also known as NHS Digital.

See the detailed coverage guide here

Trainin

4. Managi 5. Proces

). IT prof

Red little :

| ISO 27001 Coverage | |
|--|---------------|
| Casta Siecurity Standard | |
| al confidential data | |
| · · · · · · · · · · · · · · · · · · · | |
| Entra Security Readerst anding your responsibilities | |
| arong your responsioners | |
| Data Security Standard | |
| | |
| • | |
| g data access | |
| g data access | |
| Data Security Standard | |
| reviews | |
| + | |
| Data Security Standard | |
| ang to incounts | |
| Data Security Standard | |
| ty Planning | |
| + | |
| Easta Security Standard | |
| g unsupported systems | |
| Data Security Standard | |
| don and a second se | |
| + | |
| table suppliers | |
| table supprens | |
| little / no coverage Amber = Some coverage Green = Significant Coverage | |
| | |
| | |
| © 2017 Health and Social Care Information Centre. | |
| | |
| | |
| | |
| | |
| | See the c |
| | |
| | |
| | PSN |
| | Pan |
| | |
| | 1. Personal o |
| | |
| | 2.110 |
| | 2. Understand |
| | |

See the detailed coverage guide here

| Data Security Standard | |
|---|-------------------------|
| 1. Personal confidential data | |
| • | |
| Data Security Standard | |
| 2. Understanding your responsibilities | |
| • | |
| Data Security Standard | |
| 3. Training | |
| Casta Security Standard | |
| 4. Managing data access | |
| - managang unu mutan | |
| Data Security Standard | |
| 5. Process reviews | |
| + | _ |
| Data Security Standard | |
| 6. Responding to incidents | |
| • | |
| Data Security Standard | |
| 7. Continuity Planning | |
| • | |
| Data Security Standard | |
| 8. Managing unsupported systems | |
| Casta Security Standard | |
| 9. IT protection | |
| a prosecuti | |
| Data Security Standard | |
| 10. Accountable suppliers | |
| | |
| ted little = little / no coverage Amber = Some coverage | e Green = Significant C |
| | |

See the detailed coverage guide here



d little = little / no coverage Amber = Some coverage Green = Significant Coverage



Example – Levels of Data Security

- Basic level
- Secure configuration
- Boundary firewalls
- Internet gateways, access control
- Patch management
- Malware protection
- Security awareness

- "Alcatraz" Level
- ISO 27001
- CISSP qualified
- Ethical Hacking/Pen Testing
- Cryptography
- Security in SDLC
- Web Application Firewall (WAF)
- CIS Benchmarking
- Risk Frameworks
- Embedded Systems Security
- Security Evaluation Standard for IoT Platforms
- Data encryption at rest
- Data anonymisation
- "Security by Design"

Example – levels of resilience













Example – Levels of Resilience

- Basic level
- Disaster Recovery with ARC provider
- UPS
- Generator

- "Nuclear" Level
- Tertiary technical and operational redundancy
- Geographical resilience
- Local resilience networks
- Real-time dual+ running
- Multiple telephony routing from NGN and multi telephony exchanges
- Fully remote workforce

Communicate clearly about what differentiates us

TSA special Interest Group - Goal

"How do we find an easy and accessible way to communicate, to commissioners and customers, that how providers address data security and resilience is different – and their investment will be different?"



SIG Goal

- New quality rating system for data security and resilience
- Tiered standards (Good/Excellent/Outstanding?)
- Clarity for customers/commissioners
- Helping them to navigate digital transition and us to be clear of the steps we're taking



Thankyou



