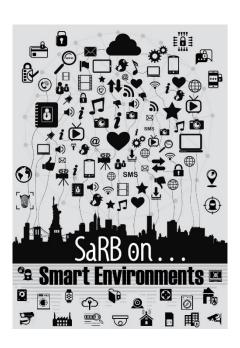
Smart Environments -

- What are they and who is responsible for Security?



Presented by :

Sarb Sembhi CISM

CTO & CISO – Virtually Informed

Joint Vice-Chair, Smart Building Group – IoT Security Foundation

Disclaimer

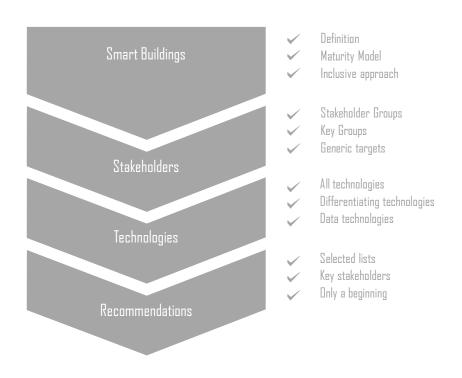
Presentation not endorsed by the IoT SF Smart Building Group

Please note that this presentation is taken from a White Paper written by James Willison and Sarb Sembhi, sponsored by Axis.

This presentation is not intended to be the work of the Smart Building Group, but a possible approach to the issues of getting started in Smart Building Security.

The Paper is available at: https://www.axis-communications.com/Smart-buildings-and-smart-cities-security

AGENDA





WHAT IS A SMART BUILDING?

"A Smart Building is one which utilises several different sensor technology systems to collect data and sharing it via a network to a unified management system to take actions or make decisions in order to provide benefits to building managers, occupants and visitors."

KEY ATTRIBUTES OF SMART ENWIRONMENTS



Connectivity
Connects to different technology systems



Sensors
where sensor technology system(s) are



Network Connected via a network



Unified System to a unified management system



Actions to take actions or make decisions in order to



Stakeholder Benefits provide benefits to its stakeholder.



Security
Security pre-requisite

The implied pre-requisite is that the whole technology that wraps around the building is secure so that it is able to function with the intended integrity, availability and confidentiality that is expected by all users.

BUT ...

"A building only becomes smart when all systems are connected so that data from them can be used to make better benefit decisions, until that point it is only a building that uses smart technologies."



SMART BUILDING MATURITY LEVELS

NFW TFCH

Levels -1. 0 and 1 to 4

TRADITIONAL Buildings that may or may not use any number of non-integrated systems controlled by facilities management teams (this is the state of most buildings of yesteryear)

Buildings that use smart technologies (this is the current state of many buildings today): without integrating them (or integrating only a few of them) and or, the benefits focus more on a single user group and or, don't provide a unified management control system



ADAPTIVE Buildings that meet the above criteria and have utilised the data to adapt to the environment





This approach has been adapted from Buckman, A.H; Mayfield, M; Stephen B.M & Beck (2014) What is a Smart Building? https://doi.org/10.1108/ SASBE-01-2014-0003; accessed 22/05/19



Stakeholders

STAKEHOLDER GROUPS

Write your relevant text here

Building-related stakeholders and groups Building & construction sub-groups

Occupant stakeholders

Product / solution / service providers

- 1 Nwners
- 2. Investors / developers
- 3. Landlord
- 4. Architects

- 1. Smart materials vendors
- 2. Consultants / building services enginers
- 3. Decommissioning consultants
- 4. Systems owners
- 5. Security advisor
- 6. Town planners
- 7. Building controls / compliance
- 8. Utilities suppliers and purchasers

- 1. Occupier / user (lessee)
- 2. Enterprise Executive Board
- 3. Emplyees
- 4 Facilities teams
- 5. Purchasino Dept.
- 6. Chief Security Officer (CSO)
- 7. IT Dept.
- 8. Chief Information Security Officer (CISO)
- 9. Data Protection Officer (DPO)
- 10. Converged Security Operations Centre
- 11. Visitors

- 1. Smart orid & energy supplier
- 2. Smart water system supplier
- 3 Predictive Al vendor
- 4. Space usage & utilisation
- 5. Surveillance vendor
- 6. Access control vendors
- 7. RMS vendors
- 8. Alarm vendors
- 9. Energy Management System
- 10. Lifts & escalator vendors
- 11. Light system vendors
- 12. Integrator
- 13. Component developers

KEY STAKEHOLDERS

Grouped generically



Owners

Forward thinking owners will create benefits for other stakeholders that can translate into additional benefits



Developers

These include those who write code libraries, as well as Apps that use API's, etc.



Integrators / Installers

This group will interpret system designs implement them, they must have the prerequisite knowledge to install securely



Specifiers

Unless a strategic view of security is specified, change may be much slower



Marketing

This group has a lot to answer for when it comes to education and complacency. They can educate consumers better



Facilities Teams

These teams operate the systems on a day to day basis, and must be adequately trained to understand any anomolies



Manufacturers

Any producer of any component, device, software or systems, must consider the required controls for security



System Designers

This group often has the overall picture that sometimes others don't at later stages, providing guidance is essential



Maintenance

Ensuring the continued secure state of a system is vital



TECHNOLOGIES FOR SMARTER SYSTEMS



Al

Artificial Intelligenc

Al seems to be the must have technology in building control systems, such that some vendors have big data analytics but are calling it Al, and making up the Al part. They are often requesting all customer data for the approach to work. Any vendor that wants all of your data, either doesn't understand the data, Al, or the model or all three.

Al as a service which can by brought in separately afterwards will be available in a few years. Where there will be a good distinct separation of data from the Al service provided.



Big Data Analytics

The Current state of most technolog

Big Data Analytics has been around long enough for mos customers and vendors to understand what the options are.

Those customers who get the most out of BDA, are those who know what they want from the analysis and can articulate it to the vendors. Many information security systems come with these tools to find anomalies and other such information that would otherwise be harder to identify.

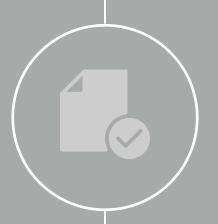


Edge Computing

At the edge of the network, device, etc.

Although there are several examples of this at the moment, this is a technology that hasn't been fully exploited today, but as it does so in the next few years, it will provide a range of capabilities that have not yet beer realised.

Edge computing will be able to take advantage of 5G and fast connections to provide localised device based decisions and actions based on more complex sensor data



Right Data

Right data and good data

In today's world of collecting all data, business face the challenge of identifying what is the right data for the right purpose, available at the right time – just in time data. Data collection will be come less important as the collection of the right data (for both compliance and business) becomes vital for quicker agile business and security decisions.



Open Data

Feeds into and out from Open Data sources.

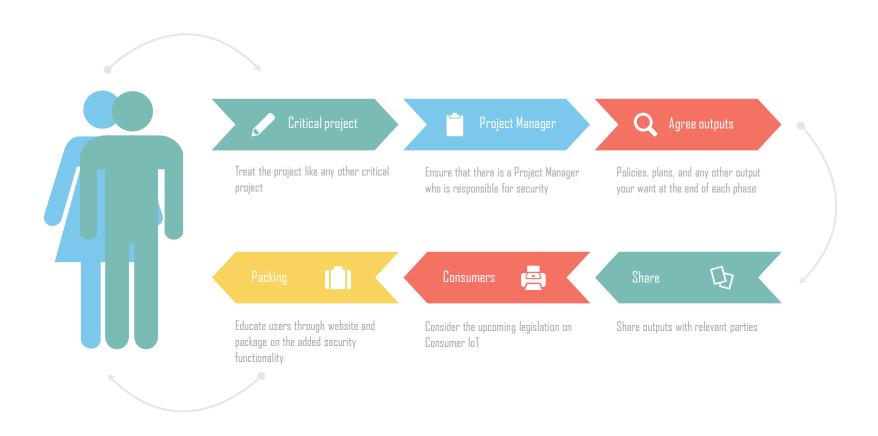
The types of and volumes of Open Data available is growing on a daily basis. This trend is likely to continue where large efficient organisations will share more and more data for interested researcher. The number of projects that will identify what constituets as useful or quality data will also increase and help the overall better use of Open Data.



Recommendations

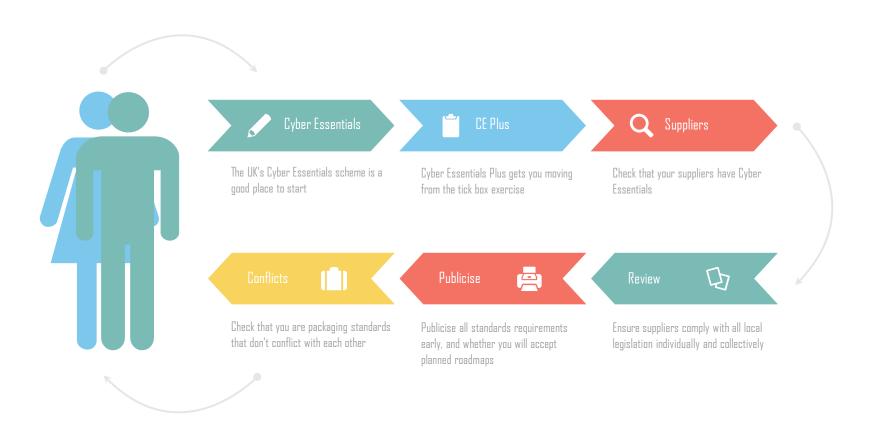
GETTING STARTED

The bleeding obvious and basics



STANDARDS AND FRAMEWORKS

There are many starting places to get you on your journey



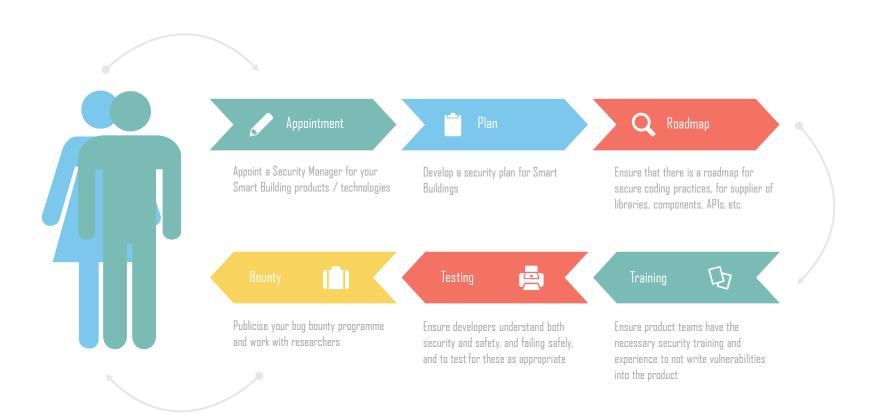
PRODUCT STRATEGY & SUPPORT

Would you buy a product with a short support plan?



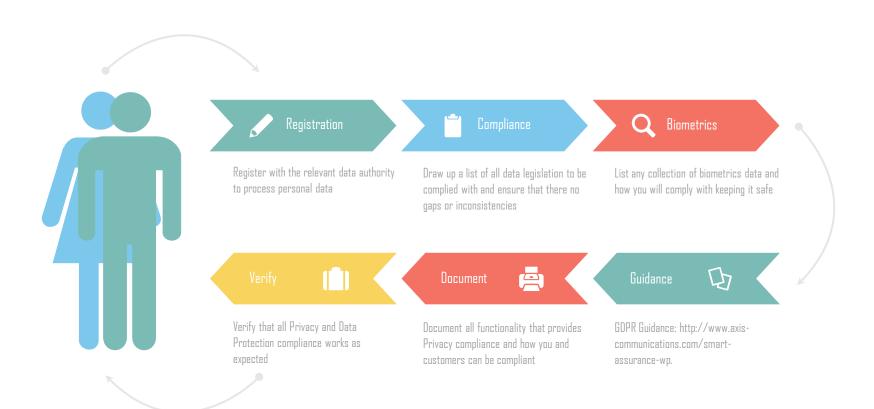
PRODUCT, SYSTEM & SOLUTION

Write your relevant text here



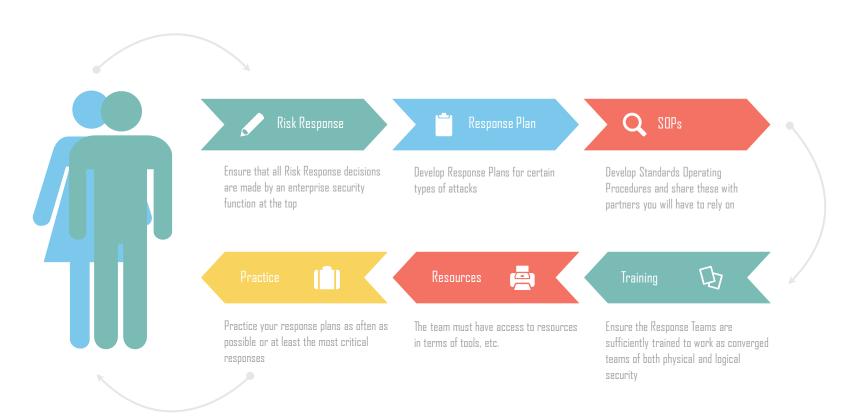
PRIVACY & DATA PROTECTION

Write your relevant text here



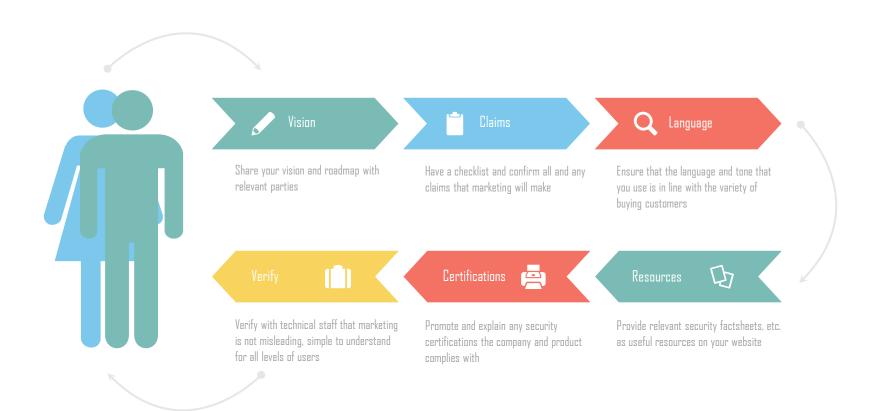
CONVERGED SECURITY

Since Filding the searce with not a Converge Security Operations Centre?



MARKETING

This is the big area that is hardly ever done right



THANK YOU VERY MUCH

Questions later