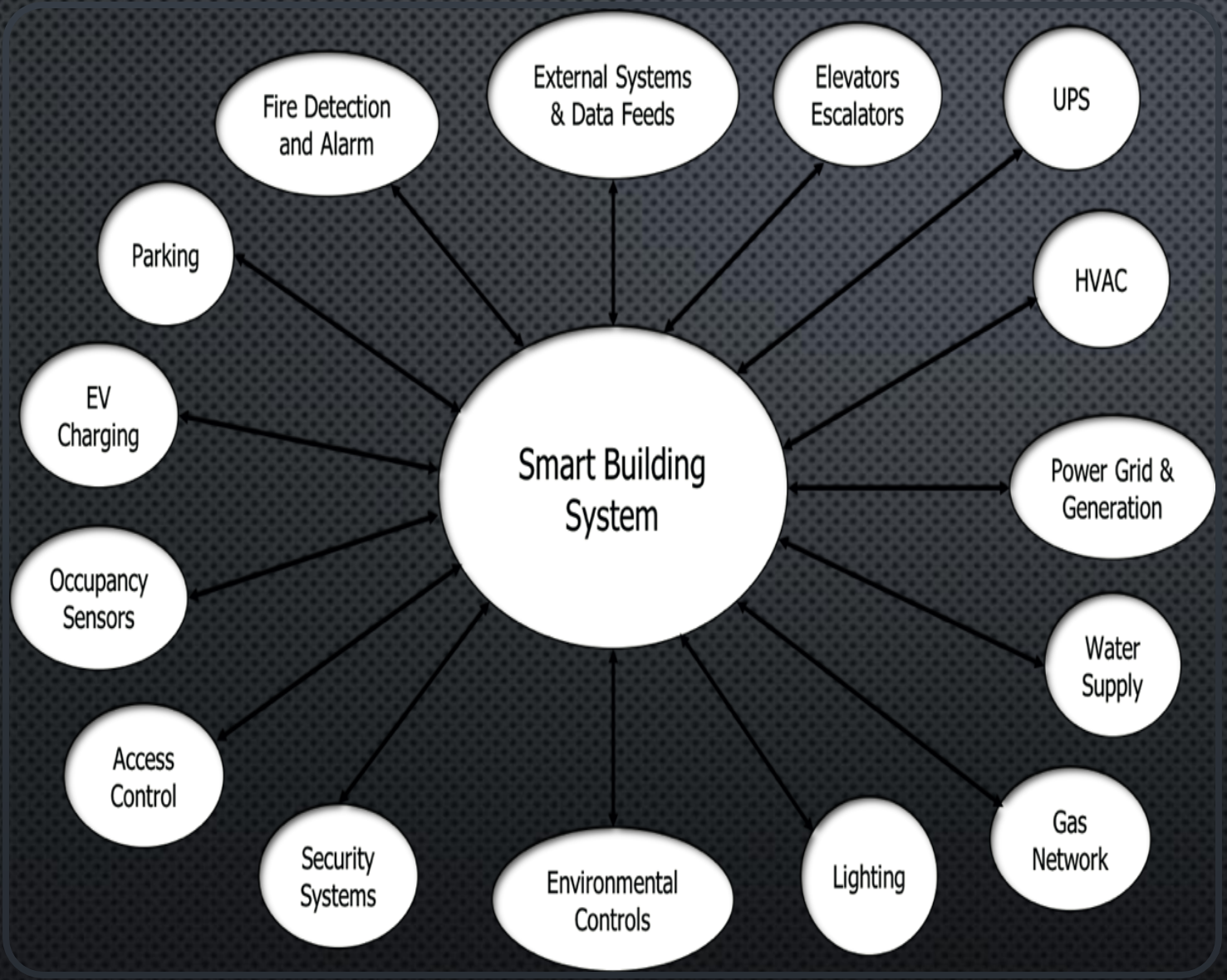
ALWAYS ON, CONNECTED EVERYWHERE: CAN WE REALLY BE SAFE?

SMART BUILDINGS….ARE THEY REALLY?

Up until recently, real estate had been terribly slow to embrace technology

Investment value was driven by location, tenure, build quality and security

Increasingly it is now driven by smart buildings, green credentials (esg) user benefits like gyms, concierge services, lifestyle, wellness options

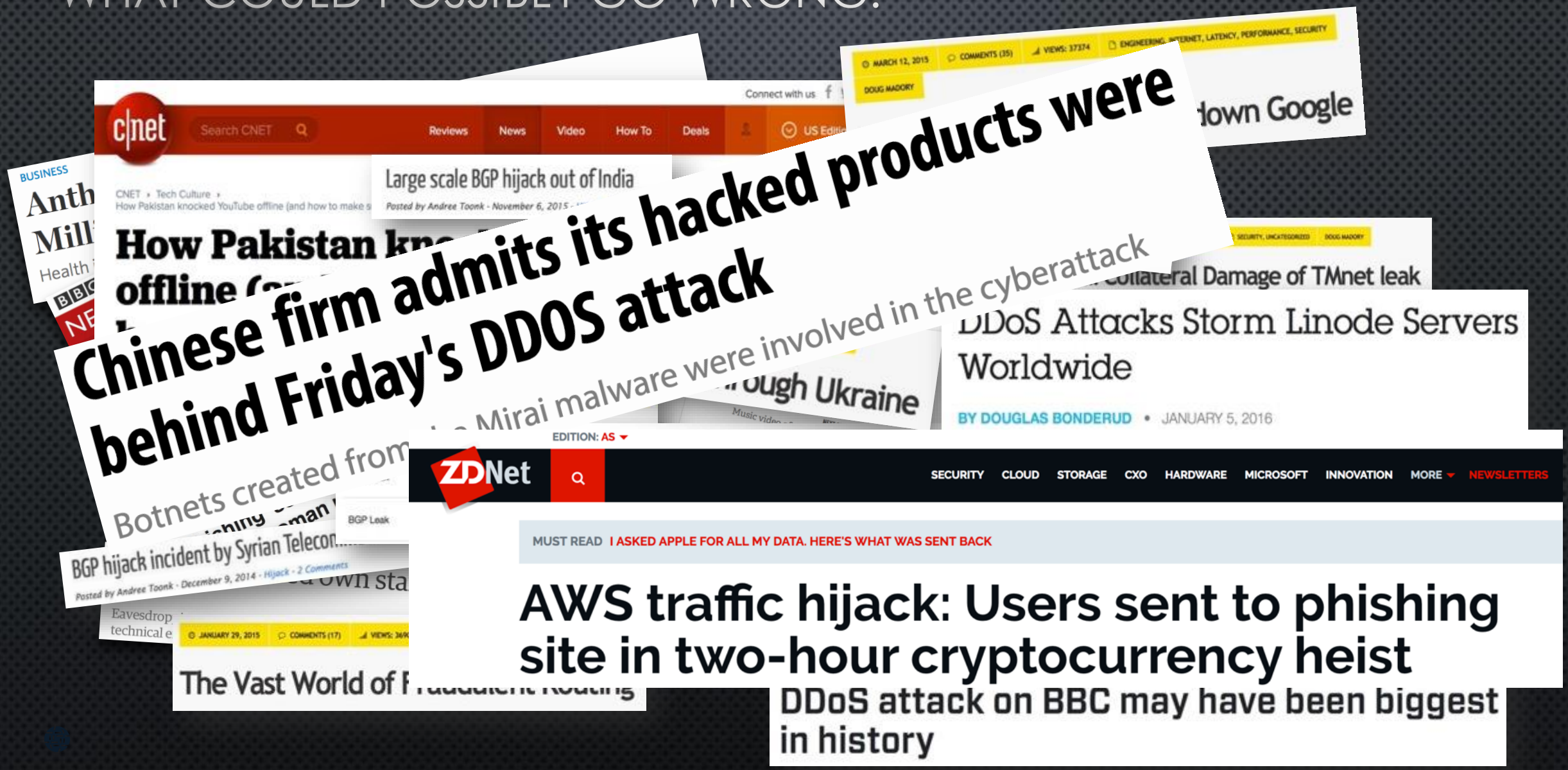


WHAT MAKES A BUILDING SMART? UNIFIED VIEW, DATA HISTORICAL AND REAL-TIME

WHY GO SMART?

- • Savings in energy and water usage and the resulting reduction in costs and carbon footprint
- • Improved working conditions, safety and security for occupants
  • Improved customer service levels
  • Visibility and management of occupancy levels
  • Optimisation of resources (physical, space and human)
  • Reduced maintenance costs

WHAT COULD POSSIBLY GO WRONG!



THE RISK TO AN ORGANISATION OR INDIVIDUAL THROUGH POOR SECURITY PRACTICE COULD IMPACT

The risk to an organisation or individual through poor security practice could impact: •

Reputation

Share price

Costs - operational, replacement, sales, legal, fines etc.

Health & Safety

New ways to gain control of your 'smart' building

- In 2017, it was revealed that criminals had managed to steal 10GB of data from a North American casino high-roller database via an internet-connected thermometer in a lobby aquarium [ref 7]. The internet-connected fish tank allowed it to be remotely monitored, automatically adjust temperature and salinity, and automate feedings.

BEST PRACTISE

- Management Governance
  • RiskAssessment• Threat Modelling• Security by Design (throughout the enterprise and system of systems) and leveraging Defence in
- Depth [ref 13 & 14]
  • Procurement (specifying security requirements for products) • Supply Chain Processes (ensuring security is maintained throughout and at source) • Secure Implementation Processes• Testing and Validation
  • Secure Maintenance and Lifecycle Management (including security software updates)
  • Training for system administrators and an enterprise monitoring plan to watch for suspicious
- events within the building network • Detection of Anomalies and Events• Continuous Security Monitoring
  • Incident response plan to effectively respond to cyber security incidents as they occur• Vulnerability Disclosure• Recovery and Resilience processes and plans to restore services in the event of a security event
  • Physical access controls (PACS) to provide wider visibility across the physical and electronic space

THREAT MODELLING

- • Deployment of hardened gateway platforms
  • Logging and auditing of security events
  • Encryption, authentication and integrity protection for communications • Tamper alarms
  • Patching processes
  • Configuration management
  • Network segmentation
  • Zero-trust configurations
  • Access controls
  • Service level agreements

CONCLUSION

Support from the Board and Executive Directors
A model of governance that empowers the central team and involves the business owners

Cybersecurity best practices that are part of the requirements and budget for the design, build and operations of the facility

Implementation of governance and security best practice across your organisation and supply chain with the cooperation of your customers, business partners and suppliers

Collaboration and adoption of cyber security responsibilities by a whole range of stakeholders