CREST
CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

UNIVERSITY OF PORTSMOUTH

Building Management Systems: Organisational Security, Context, and Convergence

Emma Boakes
University of Portsmouth

Real World Context

- Increased connectivity of physical systems.
- Implications of attacks
- Groups interested in targeting such systems *(Symantec, 2019)*
- Number of incidents increasing *(Symantec, 2019; Ponemon Institute, 2018)*
- Added complexity for organisations
  - Know the attack surface? *(Ponemon Institute, 2018)*
  - Resources? *(Ponemon Institute, 2018)*

Real World Context

DDoS attack halts heating in Finland amidst winter

KIM ZETTER SECURITY 05.06.13 06:30 AM

RESEARCHERS HACK BUILDING CONTROL SYSTEM AT GOOGLE AUSTRALIA OFFICE

KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

05 Target Hackers Broke in Via HVAC Company

FEB 14

Cybersecurity

Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar

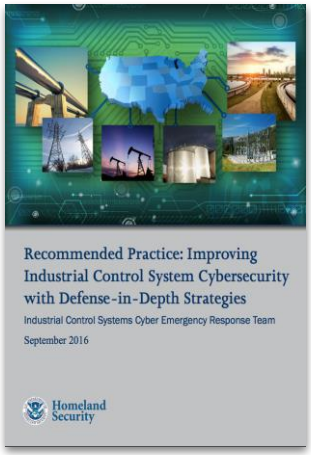
Convergence

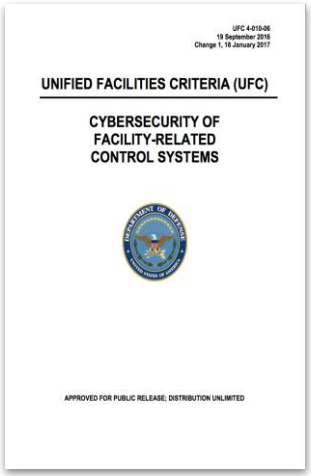
- Integration of security resources *(Tyson; 2007)*
- 57% security professionals think this is important or useful *(Dorey, Willison, Sembhi; 2012)*

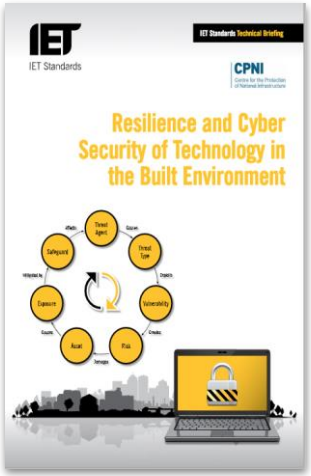
Benefits	
	➜ Cross training and communications *(Slater, 2005)*
	➜ Visibility and alignment with the business *(Ritchey, 2018)*
	➜ Prioritisation of vulnerabilities *(Willison, Sembhi and Kloet, 2012)*
	➜ Synergy of mission, efficiency and costs *(Ritchey, 2018)*

- But what type of convergence?
- How do organisations adopt a convergence approach?

Practitioner Guidance



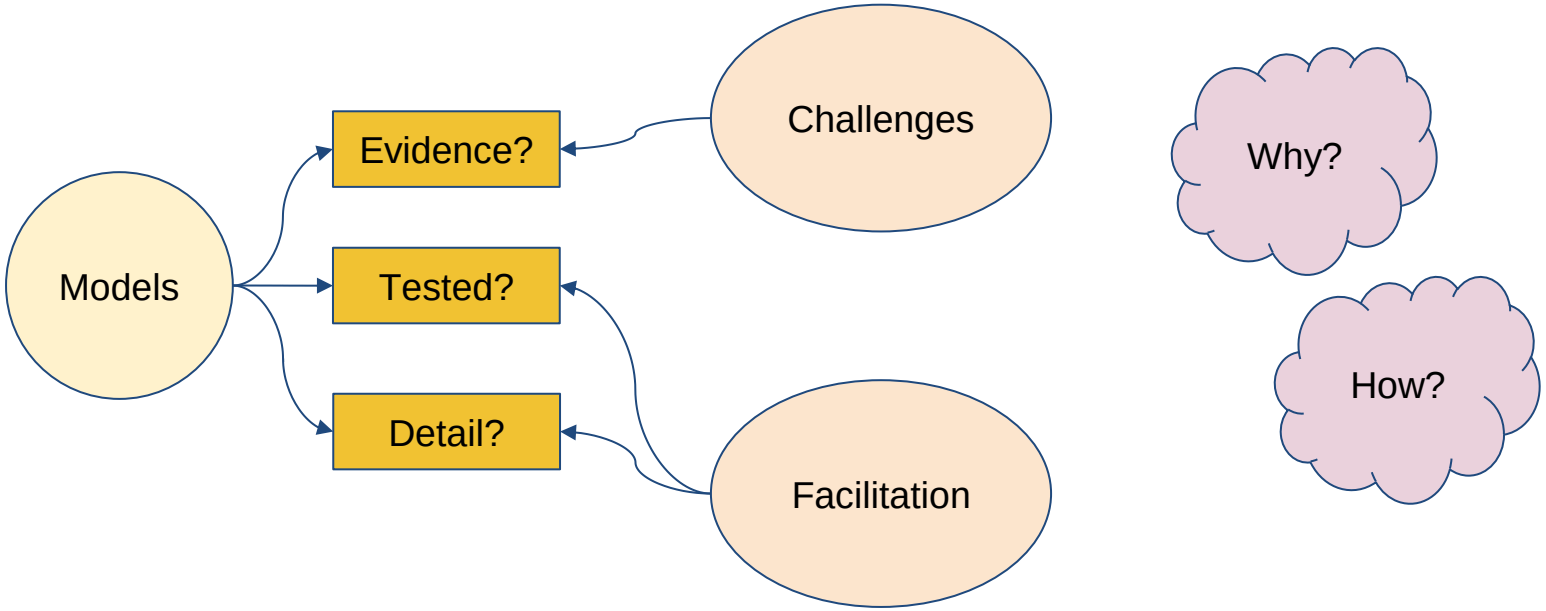




- Validity of suggestions
- Correct level of detail
- Narrow technology focus
- Complexity and overload
- Convergence?

Research Literature

- Models and frameworks
  - 3 structural converged solutions *(Rahman and Donahue, 2010)*
  - Model aligning processes *(Aleem, Wakefield and Button, 2013)*
  - Framework from risk frameworks *(Kamp, 2016)*



Initial interview study

- 5 interviews
  - 3 face to face, 2 telephone
  - Operating a converged security function
  - Variety of organisations
  - 45 minutes to 1 hour 40 minutes
- Transcription and thematic analysis

Preliminary findings

Convergence strategies

Structure: Overarching function
Operation: Forums, meetings, job design

Reach of security

Cyber, physical, personnel…
...business continuity,
...operational resilience,
...incident management

Security as a consultancy

...enabler not naysayer
...understand the business
...security service to business
...communicating security

Championing the approach

...vision
...skills to sell the idea
...set the culture

Conclusion

- Attacks exploit the gaps between security disciplines;
- Converged security widely advocated as a way of addressing this;
- Little information to assist organisations;
- Need to consider broader context;
- Preliminary findings provide some indicators of how convergence works;
- More research is needed to explore this further.

CREST
CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

UNIVERSITY OF PORTSMOUTH

Any questions?

Emma Boakes
University of Portsmouth

emma.boakes@port.ac.uk

References

- Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal*, 26(3), 236-248.
- Boyes, H. (2013). *Resilience and cyber security of technology in the built environment*. Institute of Engineering and Technology, London, UK
- BSI (2015). *PAS 1192-5: 2015: Specification for security-minded building information modelling, digital built environments and smart asset management*. Retrieved from https://www.procad.ie/wp-content/uploads/2018/02/PAS_1192_5_2015.pdf
- Dorey, P., Willison, J., and Sembhi, S. (2012). Converged Security Management Survey 2012. Retrieved from http://personal.rhul.ac.uk/vsai/149/Convergence%20Survey%20Final%20070312_V6.pdf
- Janita (2016). *DDoS Attack Halts Heating in Finland Amidst Winter*. Retrieved from http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter
- Kamp, G (2016). *Security Convergence in a Critical Infrastructure Framework and Enablers for Successful Implementation*. Masters Thesis. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/53731/2016_Kamp_CSM.pdf?sequence=1
- Krebs, B (2014). *Target Hackers Broke in Via HVAC Company*. Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
- Ponemon Institute (2018). Measuring & Managing the Cyber Risks to Business Operations. Retrieved from https://static.tenable.com/marketing/research-reports/Research-Report-Ponemon-Institute-Measuring_and_Managing_the_Cyber_Risks_to_Business_Operations.pdf
- Rahman, M., & Donahue, S. E. (2010). Convergence of corporate and information security, *International Journal of Computer Science and Information Security*, 7, (1), 63-68.
- Ritchey, D (2018). *The Unstoppable Convergence Between Physical and Cybersecurity*. Retrieved from https://www.securitymagazine.com/articles/88847-the-unstoppable-convergence-between-physical-and-cybersecurity
- Robertson, J. and Riley, M (2014). *Mysterious '08 Turkey Pipeline Blast Opened New CyberWar*. Retrieved from https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
- Slater, D (2005). *Physical and IT Security Convergence: The Basics*. Retrieved from https://www.csoonline.com/article/2117824/physical-and-it-security-convergence--the-basics.html
- Symantec (2019). Internet Security Threat Report, Volume 24, February 2019 . Retrieved from https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf
- Tyson, D. (2007). Security convergence: Managing enterprise security risk. Elsevier.
- Willison, J., Sembhi, S., and Kloet, F. (2012) Security Convergence and FMs: the Learning Curve. Retrieved from https://www.ifsecglobal.com/uncategorized/security-convergence-and-fms-the-learning-curve/
- U. S. Department of Defense (2017). *Unified Facilities Criteria (UFC): Cybersecurity of Facility-Related Control Systems*. Retrieved from http://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2016_c1.pdf
- US Department of Homeland Security (2016). *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. US-CERT Defense In Depth*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- Zetter, K (2013). *Researchers Hack Building Control System and Google Australia Office*. Accessed on 25th March 2019 from https://www.wired.com/2013/05/googles-control-system-hacked/
- Zetter, K (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.* Accessed on 25th March 2019 from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/