HOW SECURE IS HOME: ASSESSING HUMAN SUSCEPTIBILITY TO IOT THREATS

EMILY KATE PARSONS, EMMANOUIL PANAOUSIS, AND GEORGE LOUKAS, UNIVERSITY OF GREENWICH

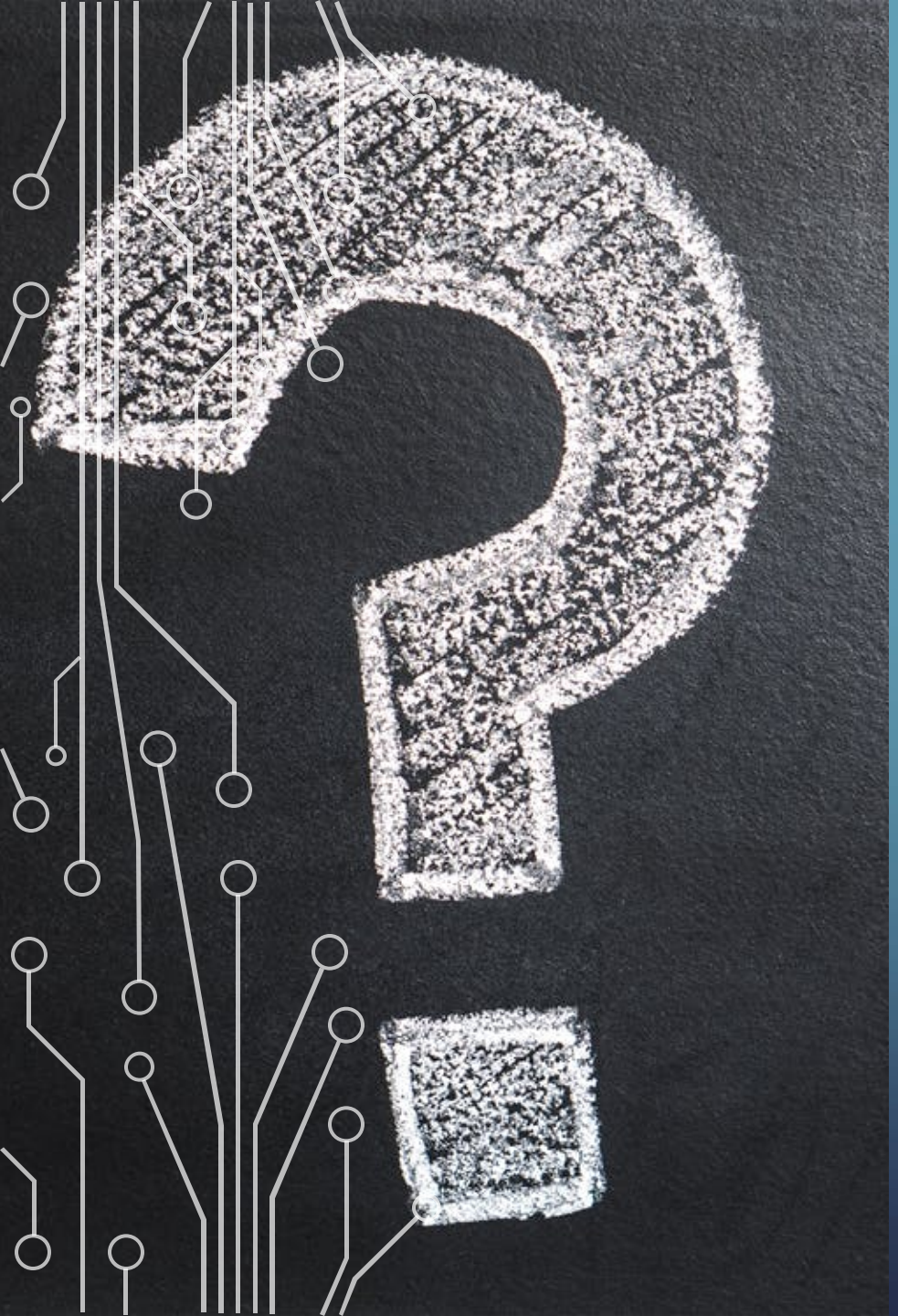
24TH PAN-HELLENIC CONFERENCE ON INFORMATICS (PCI 2020)

THE WORK FROM HOME-REMOTE OFFICE (WFH-RO)

- COVID-19 has forced many organisations to let employees work from home.
- They are now are reaping its operational benefits.
- The work from home environment can contain both personal and business orientated assets.

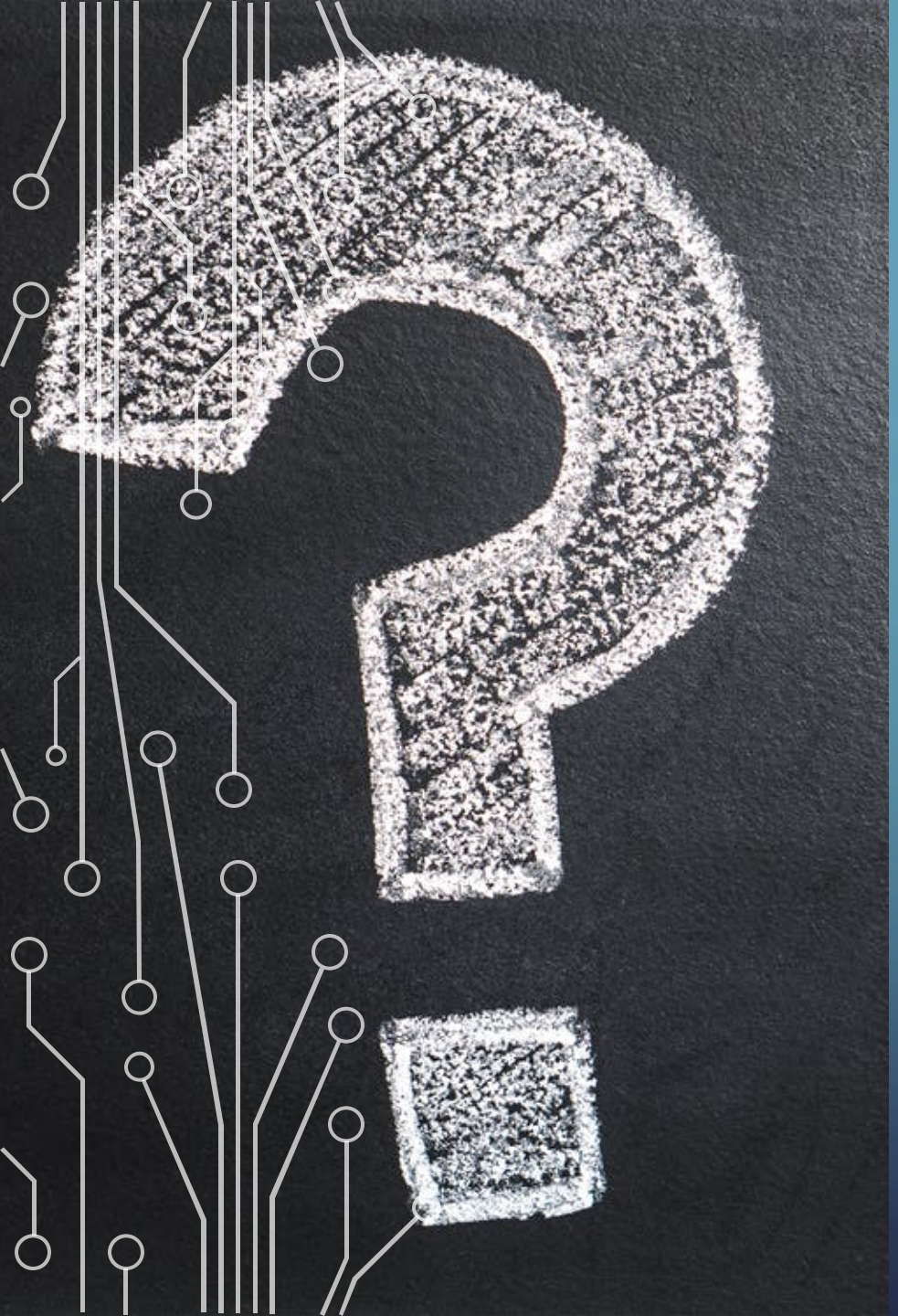
THE DECENTRALISATION OF RISK AND THE INTERNET OF THINGS

- IoT devices within the home may end up being potential targets.
- Avast [1] found that over 40% of worldwide smart homes contain least one vulnerable device.
- Bitsight [2] found that the Mirai malware was 20 times more likely in WFH-RO networks.



THE PROBLEMS

- **How can cyber risk be modelled within domestic environments?**
  - How can the work from home environment be modelled in relation to risk?
  - **How can we model the human factors?**
  - How can we assess the risk of IoT within the WFH-RO?



PROBLEMS- DECENTRALISATION, IOT, WFH-RO AND HUMANS

- Decentralisation within the WFH-RO makes it harder to quantify the threats towards an organisation.
- Part of this decentralisation comes in the form of unregulated IoT devices and user behaviour.
- **The road to becoming self-secure.**

RELATED WORK – RISK ASSESSMENTS IN IOT

- Various frameworks have been created:
  - IoTRiskAnalyzer. [3]
  - Graph theory. [4]
  - Risk analysis of individual devices. [5] [6]
- Other frameworks start to focus on the human factors:
  - OCTAVE Allegro. [7]
  - Information security risk. [8]

RELATED WORK – USER BEHAVIOUR AND ATTITUDES WITHIN IOT

- There are some key themes that we found within the related work:
  - There is exponential growth and normalisation of IoT devices with a large variety of devices being found in homes. [9]
  - Many users will undervalue personal data. [10]
  - Others feel there are no significant risks within IoT. [11]
  - Innovate technology and security are not treated the same.

OUR APPROACH - SMART HOME BEHAVIOUR AND ATTITUDE RISK MODEL (SH-BARM)

- **We focus on the user's ability to increase risk.**
- Modelling behaviour in relation to risk and start assessing risk within the domestic environment.
- We used several papers to build identify various behaviour. [12] [13] [14]
- How can end user's behaviour increase and decrease the expected loss within the home?

HOW DOES USER BEHAVIOUR AFFECT CYBER RISK MODELLING?

Expected Loss =

Likelihood of Occurrence x Attack Success x

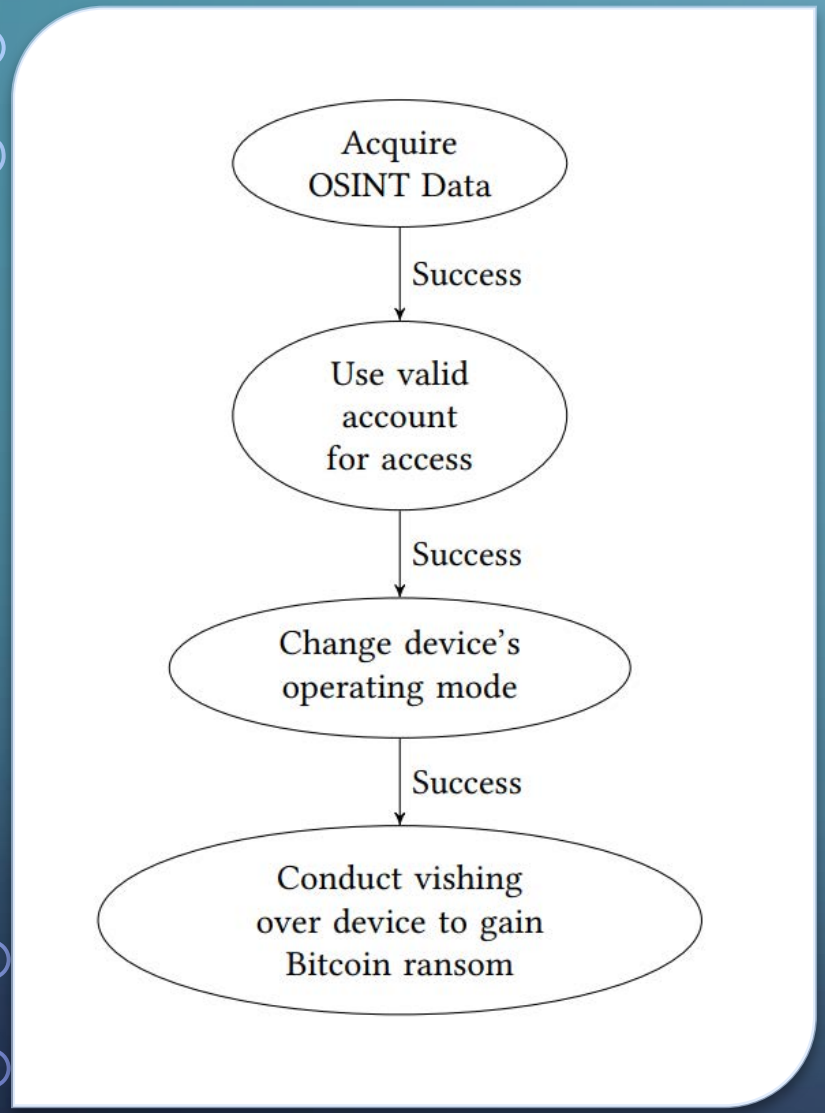
Potential Impact (1- Efficiency of Safeguards)

HOW DOES USER BEHAVIOUR AFFECT CYBER RISK MODELLING?

Likelihood of Attack Occurrence	Attack Success Rate	Potential Impact	Efficiency of Safeguards
Risk Appetite	Risk Perception	Types of Impact	Implementation Level
Security Familiarity	Risk Prevention		

SH-BARM ASSESSMENT APPROACH

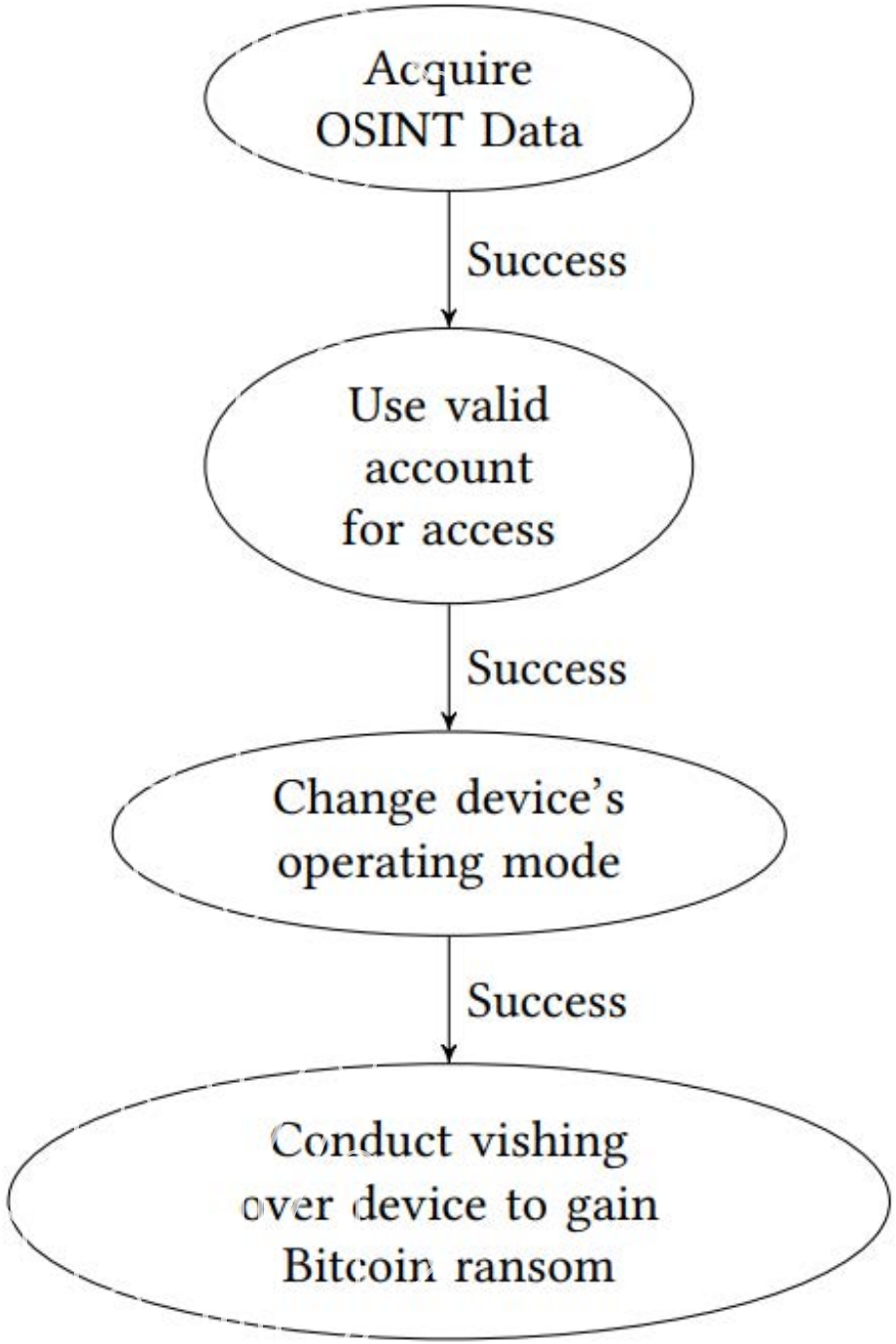
- **HSG48 [15]**
- Step 1: Look for hazardous behaviours and attitudes.
- Step 2: Decide the assets that may be harmed and the impact towards this.
- Step 3: Decide whether existing precautions are adequate or if more should be done.
- Step 4: Record findings.
- Step 5: Review and revise the risk assessment.



CASE STUDY - ESTABLISHING THE SCENARIO

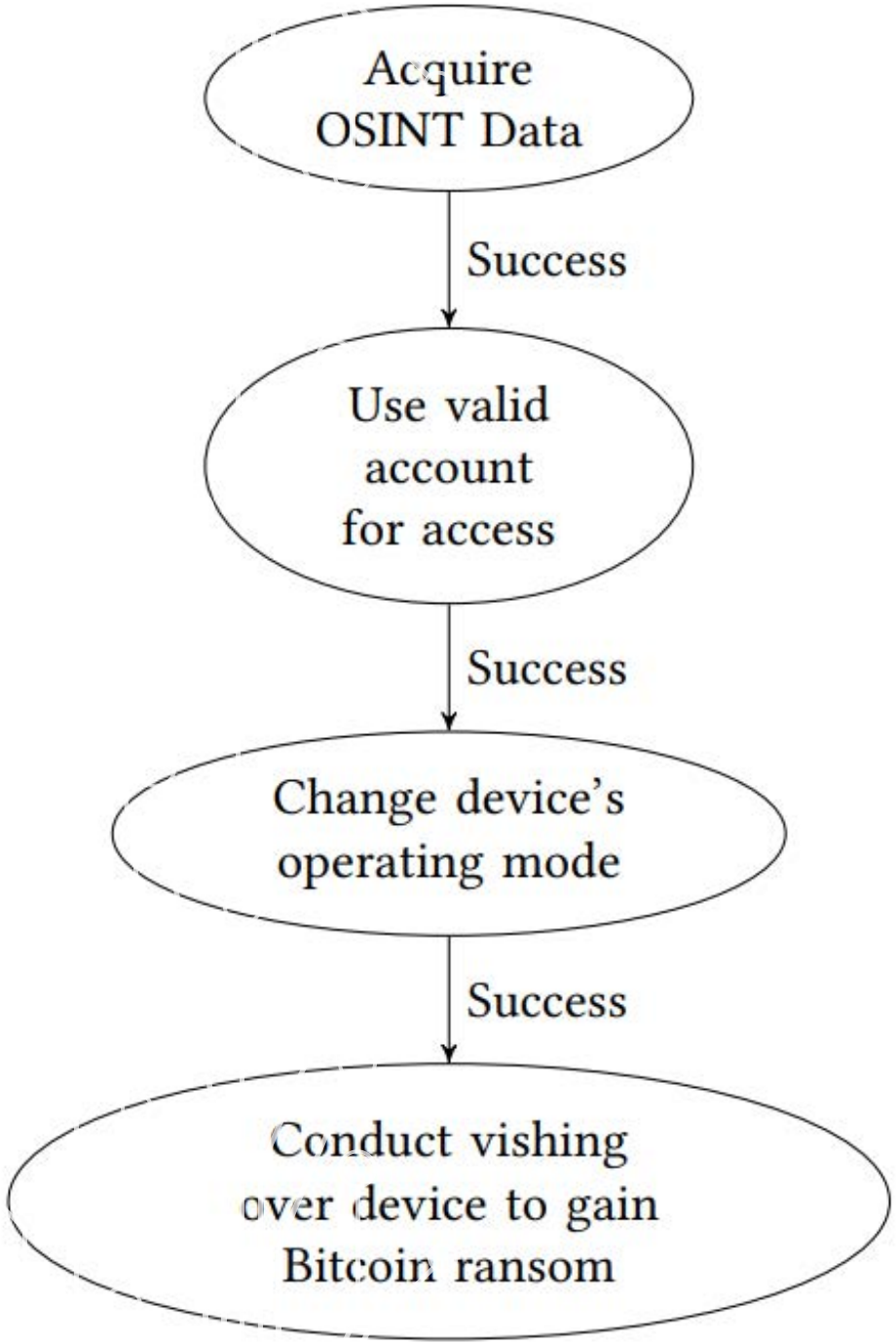
- Our case study is based on an event that was reported in 2019 where Ring Home Security systems were compromised.[1]
- Our case study suggests and examines the behaviour types that can create low, medium and high risk environments given the attack path as seen in the image.

[1] https://abcnews.go.com/GMA/News/video/terrifying-video-familys-hacked-ring-camera-system-67704081



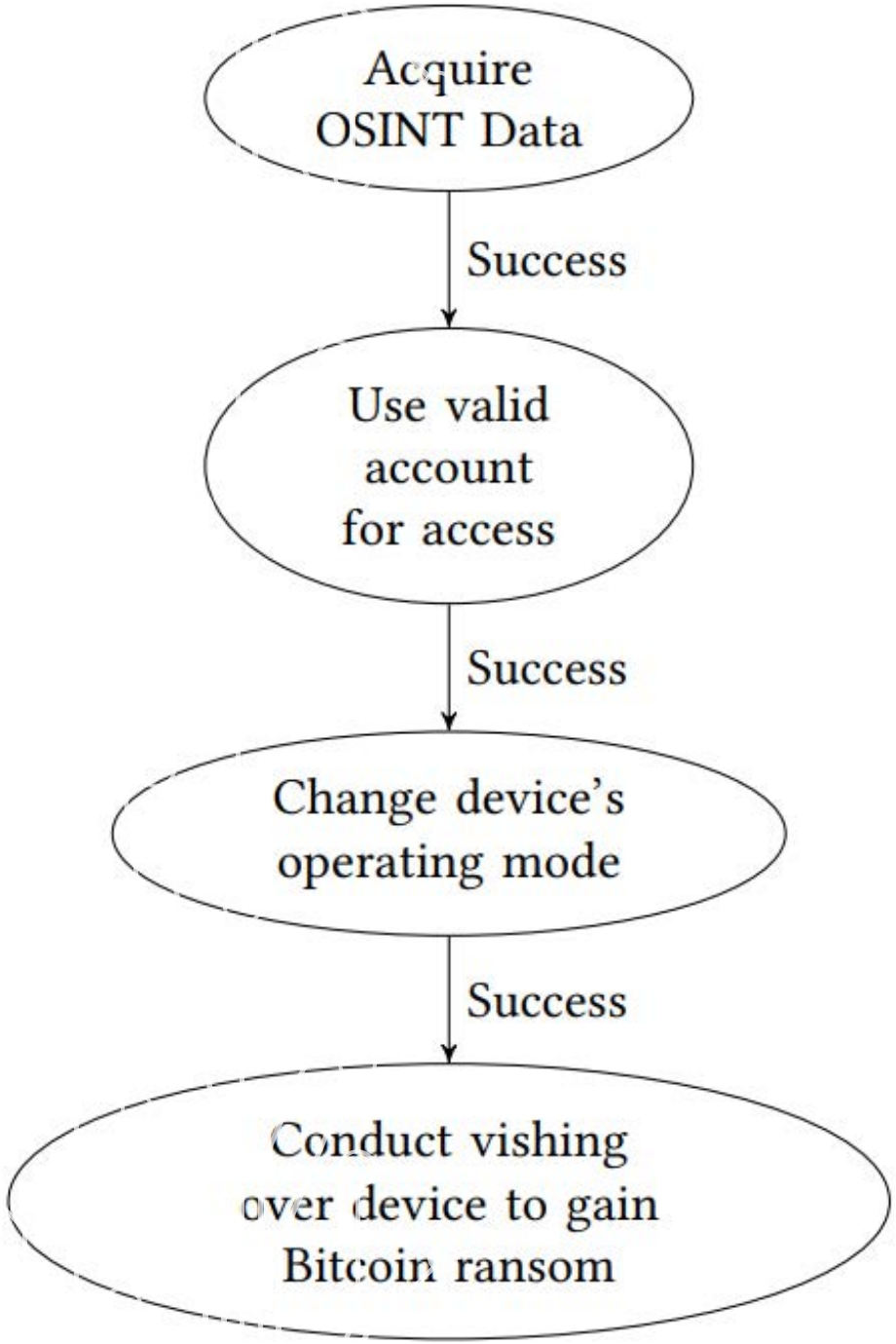
AN EXAMPLE OF A LOW RISK HOUSEHOLD TOWARDS THIS ATTACK EVENT

- A Low likelihood of attack occurrence.
  - Never reuses passwords.
  - Always uses two-factor authentication.
  - Good knowledge of social engineering.
  - Great security familiarity.
- A low attack success rate towards each attack event.
- Low impact.
- High level safeguards.



AN EXAMPLE OF A HIGH RISK HOUSEHOLD TOWARDS THIS ATTACK EVENT

- A Low likelihood of attack occurrence
  - Always reuses passwords.
  - Never uses two-factor authentication.
  - Limited knowledge of social engineering.
  - Limited security familiarity.
- A high attack success rate towards each attack event.
- High impact.
- Low level safeguards/ No safeguards.



AN EXAMPLE OF A MEDIUM RISK HOUSEHOLD TOWARDS THIS ATTACK EVENT

- A moderate likelihood of attack occurrence.
  - Reuses passwords.
  - Rarely uses two-factor authentication.
  - Great knowledge of social engineering.
  - Moderate security familiarity.
- A varied attack success rate towards each attack event.
- Varied impact.
- Varied level safeguards.

CONCLUSIONS AND CHALLENGES

- Human behaviour is always changing and may never be the same each time.
- SH-BARM is a method to start formulising and identifying negative, risk causing behaviours which can then be dealt with appropriately.

FOR THE FUTURE

- **How can risk be modelled within domestic environments?**
- To develop a risk assessment and mitigation framework for the home which provides metadata to assess and improve security within the domestic environment.
- This includes creating a risk tool which follows our framework and will:
  - assess the risk of an environment providing insight into risky user groups and assets.
  - aid users to choose the best safeguards based on various factors.

REFERENCES

- [1] Avast. Avast smart home security report 2019, 2019. https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf. Online; accessed 19-09-2020.
- [2] Dan Dahlberg. Identifying unique risks of work from home remote office networks. Online; accessed 19-09-2020.
- [3] Mujahid Mohsin, Muhammad Usama Sardar, Osman Hasan, and Zahid Anwar. Iotriskanalyzer: A probabilistic model checking based framework for formal risk analytics of the internet of things. IEEE Access, 5:5494–5505, 2017.
- [4] VL. Shivraj et al. A graph theory based generic risk assessment framework for internet of things (iot). In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pages 1–6. IEEE, 2017.
- [5] Yan Huang, Xin Guan, Hongyang Chen, Yi Liang, Shanshan Yuan, and Tomoaki Ohtsuki. Risk assessment of private information inference for motion sensor embedded iot devices. IEEE Transactions on Emerging Topics in Computational Intelligence, 2019.
- [6] Tzu Wei Tseng, Chia Tung Wu, and Feipei Lai. Threat analysis for wearable health devices and environment monitoring internet of things integration system. IEEE Access, 7:144983–144994, 2019
- [7] Bako Ali and Ali Ismail Awad. Cyber and physical security vulnerability assessment for iot-based smart homes. Sensors, 18(3):817, 2018
- [8] Senyu Li, Fangming Bi, Wei Chen, Xuzhi Miao, Jin Liu, and Chaogang Tang. An improved information security risk assessments method for cyber-physical-social computing and networking. IEEE Access, 6:10311–10319, 2018.
- [9] Ismini Psychoula, Deepika Singh, Liming Chen, Feng Chen, Andreas Holzinger, and Huansheng Ning. Users' privacy concerns in iot based applications. In 2018 IEEE SmartWorld, pages 1887–1894. IEEE, 2018.
- [10] Junhyoung Oh, Ukjin Lee, and Kyungho Lee. Privacy fatigue in the internet of things (iot) environment. IT CoNvergence PRActice (INPRA), 6(4):21–34, 2019.
- [11] Mikael Asplund and Simin Nadjm-Tehrani. Attitudes and perceptions of iot security in critical societal services. IEEE Access, 4:2130–2138, 2016.
- [12] Alexander Kharlamov, Aakanksha Jaiswal, Glenn Parry, and Ganna Pogrebna. A cyber domain–specific risk attitudes scale to address security issues in the digital space, 2018.
- Junhyoung Oh, Ukjin Lee, and Kyungho Lee. Privacy fatigue in the internet of things (iot) environment. IT CoNvergence PRActice (INPRA), 6(4):21–34, 2019.
- [13] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny RJ Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. A taxonomy of cyber-physical threats and impact in the smart home. Computers & Security, 78:398–428, 2018.
- [14] European Union Agency for Cybersecurity. Good practices for security of iot - secure software development lifecycle. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1, Dec 2019.
- [15] HSE Books. Reducing error and influencing behaviour, 2009

THANK YOU FOR LISTENING
ARE THERE ANY QUESTIONS?