

ISSA



SYMPOSIUM 19

23 – 25 May 2018

Feedback Breakout Group 'Cyber-Security Risks in the Securities Value Chain'

Bruce Butterill, ACSDA, 25 May 2018

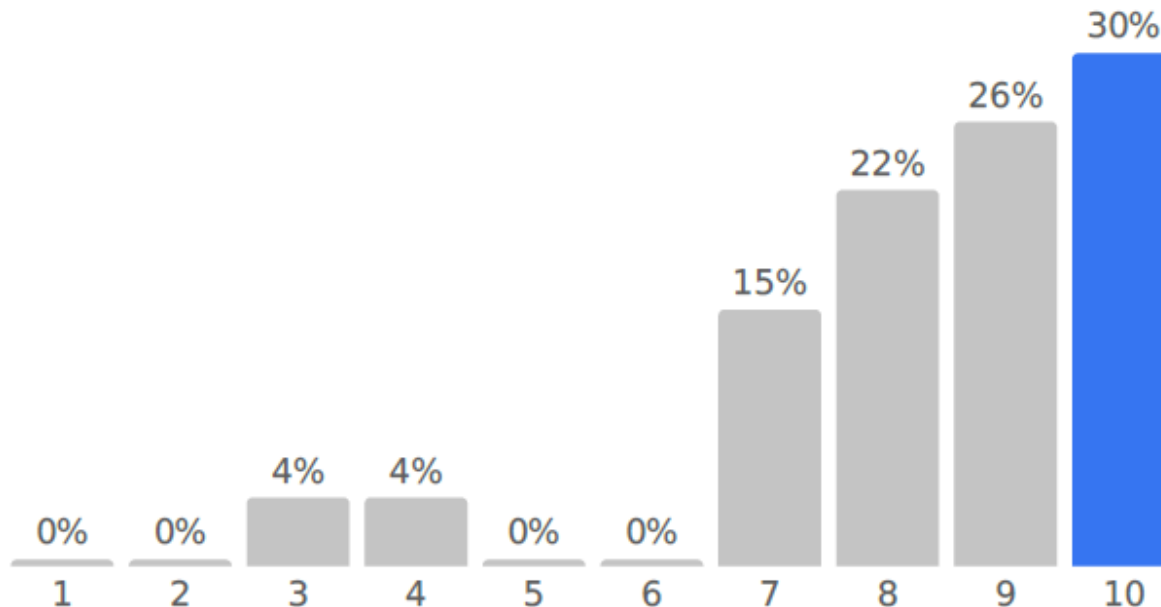
Rating poll

Risk Assessment: Q11. Disruptive / Ransom Attacks (1/6)

027

Q11a. For (A) disruptive / ransomware attack that targets a CSD/CCP utility, what's the possible market impact? (1 star = minor vs 10 stars = total market)

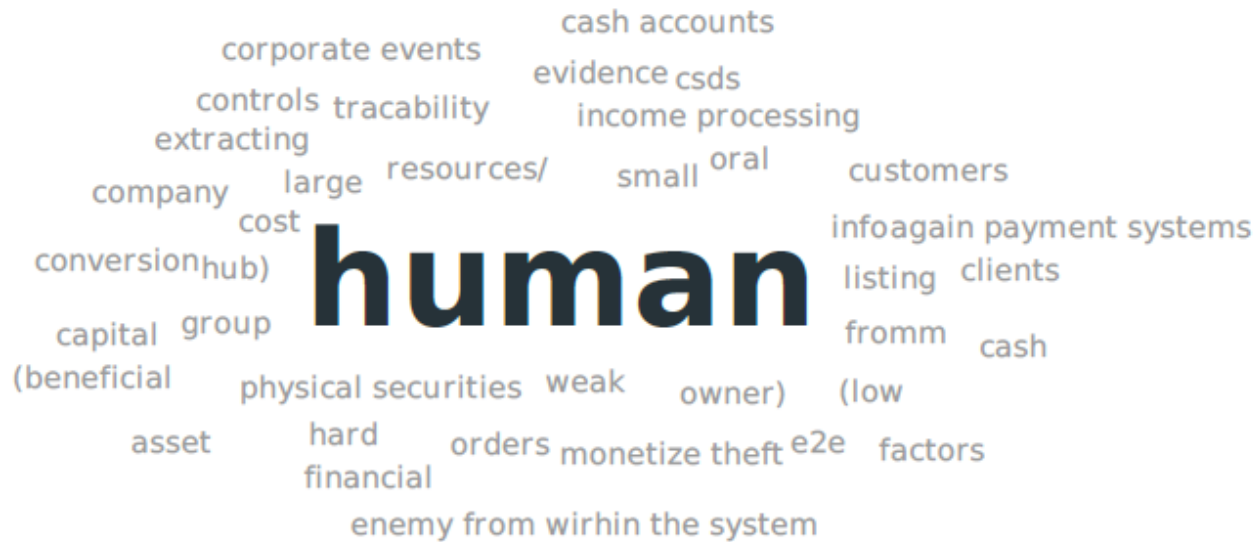
Score: 8.4



Wordcloud poll

Q4. What big susceptibility factors are missing, if any?

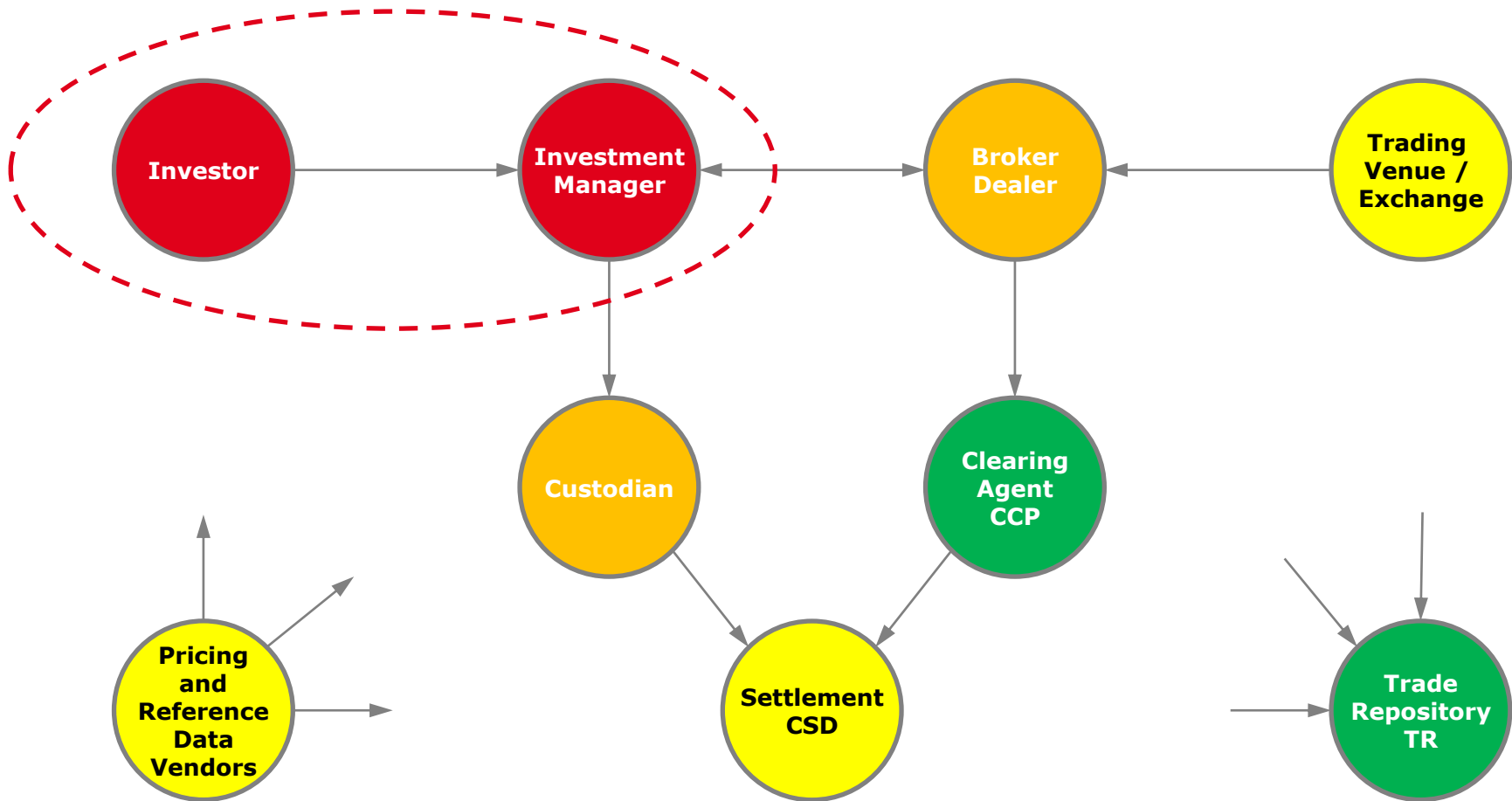
015



Agenda

- Susceptibility of Securities Value-Chain Participants
- Susceptibility Factors
- Cyber Risks
- Possible Timing
- Approaches for Adoption
- Next Steps

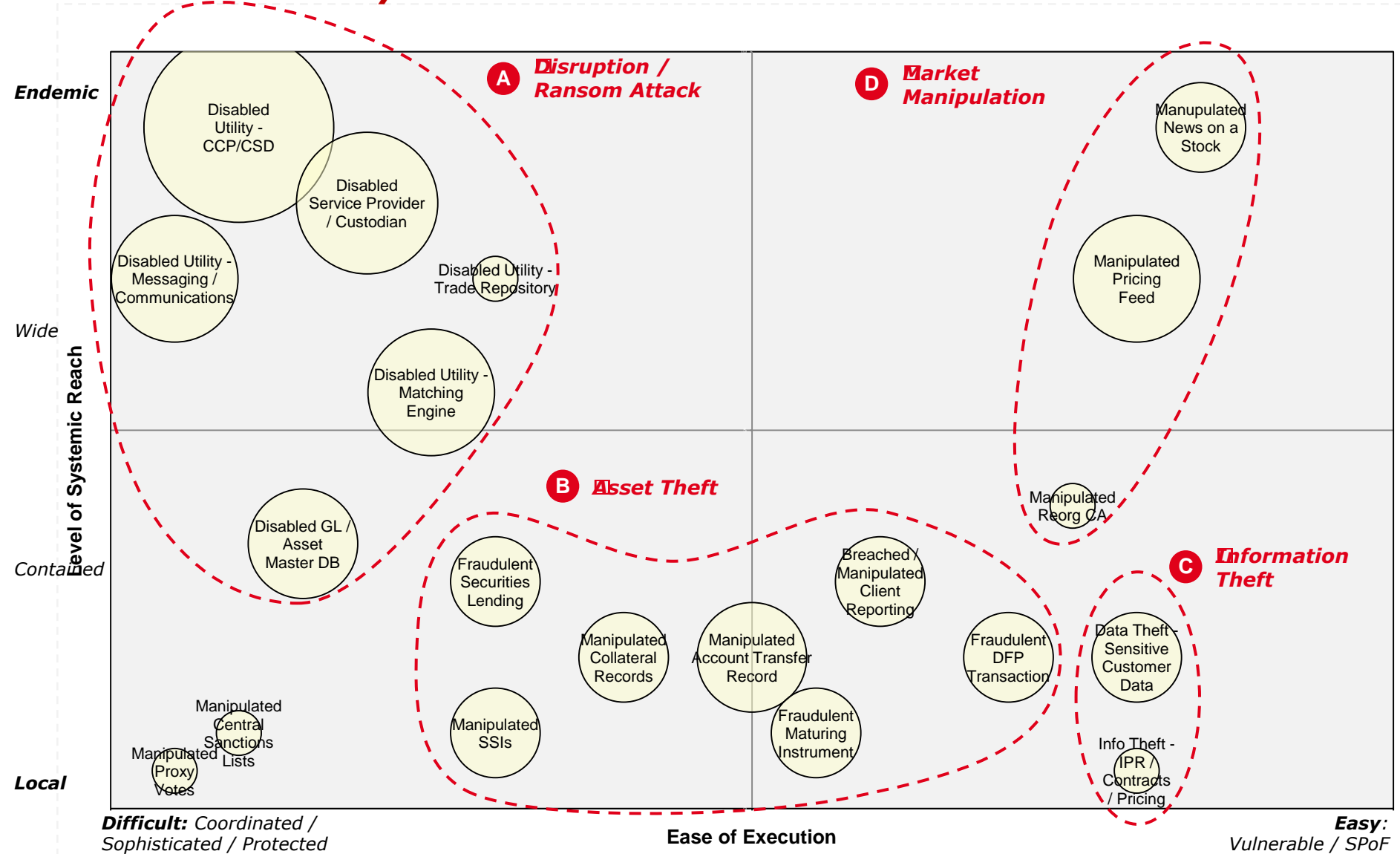
ISSA View: Susceptibility of Securities Value-Chain Participants



ISSA View: *Susceptibility Factors*

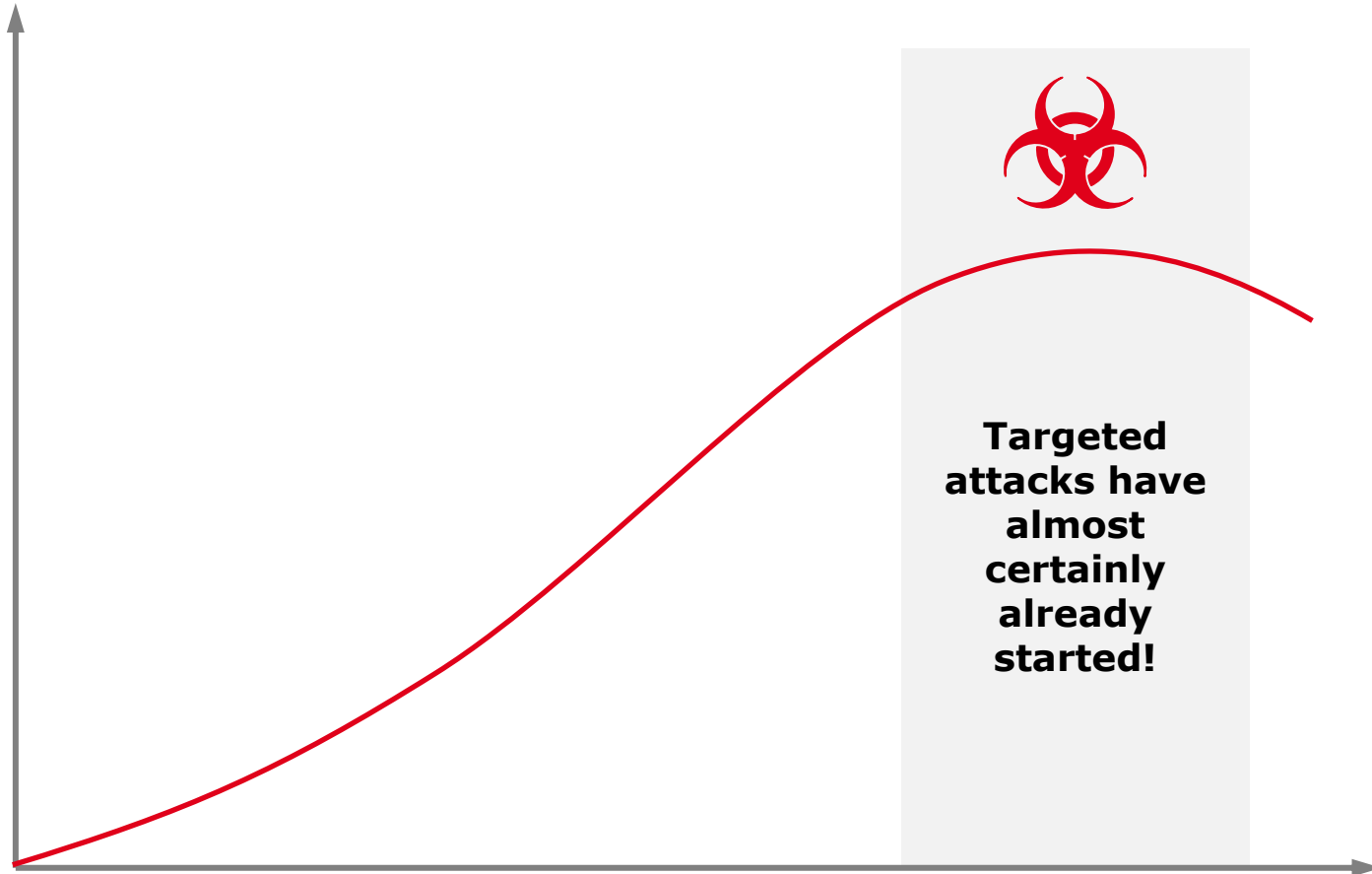
- **Concentration of very high value assets**
- **Securities is complex with many entry points, moving parts and functions**
- **Predictable asset and money movement flows - maturities and dividend schedules**
- Concentration of asset flows with high values, with bulk asset movements
- Reliance on data, from a small number of vendors, such as pricing and SSIs
- Use of omnibus vs segregated accounting that obscures end beneficiary details
- Need for internal staff to meet daily operational deadlines
- Use of HFT algorithms to automatically establish asset pricing and trading
- Contrasted use of automation and STP and manual handling

ISSA View: Cyber Risks



1. Source: ISSA WG analysis

ISSA View: Possible Timings



ISSA View: Approaches for Adoption

Approach to adopt cyber best practices	<ul style="list-style-type: none">• Don't reinvent the wheel• Leverage existing frameworks, e.g. NIST, ISO 27000 and CSP
Approach to enforcement and ensuring end client compliance to best practices	<ul style="list-style-type: none">• Encourage via pricing incentives• Risk approach through tiering• Develop relationship and manage end-points• Take up via industry groups and via market infrastructures• Invoke contractual obligations stating minimum standards
Need for industry standard incident response playbook	<ul style="list-style-type: none">• Don't reinvent the wheel• Leverage existing playbooks and runbooks, both an overall framework and adapt to your organization and business lines
Impact of new technologies, such as AI and DLT	<ul style="list-style-type: none">• Evolutionary, no clear impact yet• Liaise with the other Working Group to ensure ISSA alignment
Investments needed for adoption	<ul style="list-style-type: none">• Cost of not taking action certainly outweighs the cost of implementation

Next Steps

- Today: ISSA Symposium validated interim findings
- Working Group to convene and refine interim results, post Symposium
- Working Group to draft interim report by the end of July
- Working Group to present key finding at SIBOS [TBD]
- Working Group to create final report by year-end