Endpoint Security for Wholesale Payments

2018 CHICAGO PAYMENTS SYMPOSIUM

EMILY CARON

MANAGER, FMI RISK & POLICY

FEDERAL RESERVE BOARD

The views expressed in this presentation are those of the speaker and do not necessarily reflect the views of the Federal Reserve Board or those of the Federal Reserve System.

What is an endpoint?

- The term “endpoint” includes the participants (e.g., banks, corporations) of wholesale payment systems (e.g. Fedwire, CHIPS, Target2, CHAPS, BOJ-Net) or messaging networks (e.g., SWIFT) that can transmit and receive payment instructions on behalf of themselves or others
- Endpoint security is built upon measures taken with respect to each endpoint’s:
  - Hardware
  - Software
  - Physical access
  - Logical access
  - Organization and processes
- How many endpoints are there?
  - Thousands of endpoints, interconnected
- Risks associated with endpoint security breaches include:
  - At the endpoint level: Financial loss, reputational risk
  - At the system level: Loss of confidence in the integrity of the entire system, gridlock/economic activity impeded

Background on the CPMI report

- The Committee on Payments and Market Infrastructures (CPMI) is an international standard setting body comprised of 27 central banks representing the Americas, Africa, Asia-Pacific, Europe, and the Middle East
  - Promotes the safety and efficiency of payment, clearing, settlement and related arrangements; as a standard setter, CPMI aims to strengthen regulation, policy and practices regarding such arrangements worldwide
- Project timeline
  - September 2016: CPMI announced the establishment of Wholesale Payments Security Task Force (Task Force)
  - Through early 2017: Task Force conducted a stocktaking among CPMI members which revealed knowledge gaps and inconsistencies in approaches
  - September 2017: CPMI published a discussion note for consultation
  - November 2017: Task Force held an industry roundtable
    - 7 operators: Bank of England's RTGS, CHIPS, Euro1, Fedwire Funds, Payments Canada, TARGET2 and SWIFT)
    - 11 private sector financial institutions (e.g., banks with global payment operations)
  - May 2018: final strategy published: https://www.bis.org/cpmi/publ/d178.htm

Objectives of the CPMI strategy

- Encourage and help focus industry efforts aimed at reducing the risk of wholesale payments fraud related to endpoint security
- Promote clear, comprehensive and effective industry efforts by providing an analytical approach and common terminology
- Support industry dialogue aimed at exploring
  - Potential common issues across systems/countries
  - Potential opportunities for coordination

Overview of the CPMI strategy: seven elements

1. **Identify and understand the range of risks**
   - To ensure operators and participants understand their individual risks and their collective risk of loss in confidence in the integrity of the system
2. **Establish endpoint requirements**
   - To identify and address any gaps for prevention, detection, and response
3. **Promote adherence**
   - To provide incentives and confidence that endpoint requirements are being met
4. **Provide and use information and tools for prevention and detection**
   - To enhance current capabilities of operators and participants
5. **Respond timely to potential fraud**
   - To ensure participants and operators know who to contact and how each should respond
6. **Support ongoing education, awareness, and information sharing**
   - To promote operator and participant collaboration on procedures, processes, and resources
7. **Learn, evolve, and coordinate**
   - To monitor and to keep up with ever-changing risks

The case for flexibility

- The CPMI recognizes that there are differences among payment systems and messaging networks that need to be taken into consideration when taking concrete action to reduce the risk of wholesale payments fraud
- The seven elements of the strategy describe what should be achieved at a high level, in order to allow payment systems and messaging networks to reflect the uniqueness of each system and jurisdiction, including the legal, regulatory, operational and technological structures and constraints under which they operate
- The report includes non-prescriptive points for consideration intended to inform operators and participants of payment systems and messaging networks on how they could approach each of the seven elements
- ***But flexibility should not lead to inaction or slow progress***

Next steps: promote and monitor

- Operators, participants, and other relevant private-sector and public-sector stakeholders in each jurisdiction:
  - Need to take ownership for developing and carrying out an appropriate action plan for its jurisdiction
- CPMI, as a committee, has committed to support the strategy by:
  - Promoting and monitoring timely progress among its members
  - Supporting cross-system and cross-country coordination
  - Promote global awareness and support operationalization of the strategy
- The Governors of the Global Economy Meeting have publically committed to put the strategy into practice within their institutions and jurisdictions
- Each CPMI member has committed to support the strategy by:
  - Promoting and monitoring progress in its respective jurisdiction
  - Leveraging its roles as catalyst, overseer and/or supervisor, and operator

Federal Reserve staff actions

- Press release: “Federal Reserve Board welcomes release of global strategy for reducing wholesale payments fraud” (May 8, 2018)
  - https://www.federalreserve.gov/newsevents/pressreleases/other20180508a.htm
- Internal and domestic coordination
  - Engagement among policy and supervisory staffs at the Board and Reserve Banks
  - Building awareness among other domestic banking supervisors
  - Discussing ways to coordinate among stakeholders to monitor progress in the U.S.
- Contributions to international outreach efforts

Annex 1

Seven elements of the CPMI strategy for reducing the risk of wholesale payments fraud

Elements 1 and 2

1. **Identify and understand the range of risks.** The operator and participants of a wholesale payment system and those of a messaging network should identify and understand the risks related to endpoint security that they face individually and collectively, including risks related to the potential loss of confidence in the integrity of the payment system or messaging network itself.

2. **Establish endpoint security requirements.** The operator of a wholesale payment system or a messaging network should have clear endpoint security requirements for its participants as part of its participation requirements. Such requirements should include those for the prevention and detection of fraud, for the immediate response to fraud and, when appropriate, for alerting the broader wholesale payments network community to evolving fraud threats. In addition to the requirements established by the operator of a wholesale payment system or a messaging network, each participant of the payment system or messaging network should identify and establish its own, supplemental risk-based endpoint security arrangements as needed.

Elements 3 - 5

3. Promote adherence. Based upon the understanding of the risks and the endpoint security requirements of a wholesale payment system or a messaging network, the operator and participants of the payment system or messaging network should have processes as necessary to help promote adherence to their respective endpoint security requirements.

4. Provide and use information and tools to improve prevention and detection. The operator and participants of a wholesale payment system or a messaging network should support the provision and use of information and tools that would enhance their and each other's respective capabilities to prevent and to detect attempted wholesale payments fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible.

5. Respond in a timely way to potential fraud. The operator and participants of a wholesale payment system or a messaging network should have procedures and practices, and deploy sufficient resources, to respond to actual or suspected fraud in a timely manner. This includes, where possible and appropriate, supporting the timely initiation and communication of, and response to, a request to take action concerning a potentially fraudulent payment instruction when detected. Such procedures and practices should not alter or affect the finality of any payment that has already been settled.

Elements 6 and 7

6. **Support ongoing education, awareness and information-sharing.** The operator and participants of a wholesale payment system or a messaging network should collaborate to identify and promote the adoption of procedures and practices, and the deployment of sufficient resources, that would support ongoing education, awareness and, to the extent appropriate and legally permissible and feasible, information-sharing about evolving endpoint security risks and risk controls.

7. **Learn, evolve and coordinate.** The operator and participants of a wholesale payment system or a messaging network should monitor evolving endpoint security risks and risk controls, and review and update their endpoint security requirements, procedures, practices and resources accordingly. In addition, the operators and, to the extent practicable, participants of different wholesale payment systems and messaging networks should seek to coordinate approaches for strengthening endpoint security across systems and networks in order to achieve potential efficiencies where possible and appropriate. Similarly, regulators, supervisors and overseers of wholesale payment systems and messaging networks and participants of wholesale payment systems and messaging networks should review and update their regulatory/supervisory/oversight expectations and assessment programmes as appropriate to reflect the evolving risk mitigation strategies.