The heightened threat of cyber attacks is fueling payment losses – how should your business respond?

April 2018
The heightened threat of cyber attacks is fueling payment losses — how should your business respond?

Why is the risk of a cyber attack — and the associated losses — on payments greater than ever before?

Losses from cyber attacks on payment systems — both financial and reputational — are increasingly costly, happening more frequently and are under more scrutiny from customers, regulators, investors and media.

Share prices of impacted companies dropped an average of 5% after a cyber event was disclosed, and over 30% of customers impacted by the breach ended their relationship with that organization — weak security postures are no longer acceptable.¹

Cyber attacks are more sophisticated and now target the entire payments life cycle. Silos that exist between lines of business, payment operations (across payment types, business functions and geographies), cybersecurity, risk, compliance, technology, treasury and business continuity hamper the closely coordinated response needed to prevent, detect and respond to attacks.

In response to the business risks from cyber attackers who seek to harm or disrupt the payments system, perpetrate fraud and/or gather intelligence, regulators, industry groups and payments utilities have issued enhanced cybersecurity standards. Among these are the Federal Financial Institutions Examination Council (FFIEC), National Institute of Standards and Technology (NIST), Society of Worldwide Interbank Financial Telecommunication Customer Security (SWIFT), the Federal Reserve Board (FRB) and Office of the Comptroller of the Currency (OCC).

Evolving requirements and the fast pace of technological change necessitate a coordinated, proactive industry response in identifying emerging risks. Industry initiatives, such as those undertaken by the Financial Systemic Analysis & Resilience Center (FSARC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) Cyber-Attack Against Payment Systems exercises have laid the groundwork for the needed coordination between firms within the payments space and enhanced resilience within each firm.

What are the key takeaways?

• Rapid change in the payments space, including the emergence of Venmo, Apple Pay, blockchain payments and Zelle, as well as the ongoing development of real-time payments, has disrupted the model of traditional providers and forced them to provide new, innovative services creating many different avenues for attackers

• Breaking down silos, which starts with a robust operating model inclusive of governance, early warning capability and escalation protocols, is key in preventing, detecting and responding to cyber attacks

• A holistic, end-to-end view of the payments system must be taken considering key interactions, functional roles, data flows, business strategy, logic and threat management

How has the payment landscape changed?

<table>
<thead>
<tr>
<th>Organizations that experienced a cyber incident in 2017²</th>
<th>Losses related to fraudulent SWIFT transactions at India’s Punjab National Bank reporting in Feb 2018³</th>
<th>Bank executives surveyed in 2017 that rated cybersecurity as their number one concern in payments (greater than regulation or market evolution)⁶</th>
<th>Volume of global digital payment transactions by 2020⁶</th>
</tr>
</thead>
<tbody>
<tr>
<td>86%</td>
<td>$1.77b</td>
<td>65%</td>
<td>$726b</td>
</tr>
</tbody>
</table>


What does your organization need to consider across the payments life cycle?

A firm grasp on the payments life cycle, including points of failure and areas prone to attack, and key payment risks and controls, is critical in preventing a cyber attack, or, when attacks are detected, identifying impacts and contact points across business, technology, operations cybersecurity, resiliency and risk.

- Do you have an operating model and functional roles defined across the payments process and support functions?
- Do you have an up-to-date, robust and well-understood policies and procedures framework?
- Is the payment technology ecosystem security tested via attack/penetration testing or red teaming?
- Do you have end-to-end payment system fraud monitoring and cyber event logging and monitoring?
- Have you considered using a fusion center as support with fraud and cyber event monitoring?
- Do you have sufficient fraud, cybersecurity and risk capability to appropriately monitor and investigate issues?
- Have you mapped end-to-end data flows?
- Have you considered cross-system, cross-subprocess functional role segregations of duties?
- Are intra-and intersystem layer controls (e.g., interface, application, operating system, database) tested?

What does your organization need to consider across the payments life cycle?

1) Onboarding
- Is there a framework to define, categorize and risk assess payment types?
- Is there a defined payments strategy that covers cyber?

2) Origination
- Are anti-money laundering/know-your-customer controls embedded consistently across channels and payment types?

3) Validation
- To what extent is validation automated?
- Has a risk assessment been performed to identify the validation necessary for different payment types?

4) Processing
- How secure is the business logic used to process payments?
- How frequently is this revalidated and/or modified?

5) Clearing/Settlement
- Have you considered how upstream controls impact compensating clearing/settlement controls?

6) Confirmation
- When do you consider a payment to be “complete” and no longer a risk?

- Is there a cyber incident response plan in place that covers cyber attacks on the payments system?
- Have you completed an end-to-end risk and resiliency assessment?
- Have you performed an exercise to test your resiliency plans and procedures?

---

Bringing it all together

1. Security and fraud monitoring
   Increased need for certified fraud investigators and cybersecurity personnel to monitor things like authentication measures, 3D security, tokenization, biometrics, payment system logs, business logic and cyber threats

2. Risk and resiliency
   Confirming payments risk and resiliency are appropriately managed, an end-to-end assessment should cover user access, IT security, IT process, business process and business continuity-related controls

3. Transformation
   Payment processing transformation is an essential requirement for payment firms to build a scalable infrastructure in order to support next-generation payment methods

4. System attack, penetration and red teeming
   Payment-specific red team, attack/penetration, malware, network, application and social engineering testing techniques can identify gaps in an end-to-end process when combined with other IT and business process control testing

5. Fusion center
   Many organizations are not effectively leveraging established cyber fusion centers as reporting and metrics are not always providing value to areas outside of cybersecurity. Reporting and metrics for the broader business can be pulled from the fusion center by connecting the broader business (i.e., fraud management) into the fusion center

6. Data analytics
   Payment service providers are looking at ways to leverage data analytics and predictive modeling to drive their value-added offerings for retail and corporate customers

7. SWIFT Customer Security Programme
   Member-based organizations who act as critical utilities, such as SWIFT, are increasingly issuing cybersecurity requirements their members must adhere to

What next?

1. Consider whether there is an end-to-end view of payments at your firm, and more importantly, whether the end-to-end business risks surrounding it have been appropriately identified and assessed

2. Investigate the extent to which there is a resiliency and/or continuity plan in place in the event key payment(s) systems are attacked

3. Identify whether fraud monitoring appropriately covers business logic and key data flows in and out of your firm

4. Determine whether your payments processes and systems have been appropriately tested, including the networks, applications, infrastructure, access and business processes that span the payments system

5. Develop payments-related simulations and tabletop tests to identify governance, risk, control, ownership, decision-making and operational gaps