Treasury Cyber Response – Planning for a Quick Recovery

A clear, robust recovery plan that is tested regularly is essential if companies are to meet the challenge of an increasing number and variety of cyberthreats.

Cybersecurity threats are becoming increasingly frequent and sophisticated: WannaCry and Not-Petya ransomware alone were responsible for hundreds of millions of dollars of losses in 2017. For treasurers, it's important to prepare and plan for when, not if, the next cyberattack happens. Traditionally, cybersecurity takes a

three-layered approach – protect (in order to prevent access), detect (using technological tools and specialists to identify problems as early as possible), and respond. The third of these components – the response process – often receives less attention than protection and detection. However, having a robust and well thought out response process is critical to success in the event of cyberattack where rapid and appropriate action is essential.

Managing cyber-related risks can be daunting given the technological jargon involved. However, conventional risk management principles can largely be applied. Just as every office has water sprinklers to prevent fire damage but still practices fire drills, so do all companies need to consider what will happen if their protection fails. To develop a strategic contingency plan, corporates need to follow best practices covering their planning, testing and recovery.

Back to basics – mundane but essential

During the cyber events of 2017, Citi's clients sought to take urgent action to protect their firms. However, they behaved in different ways depending on the particular scale and scope of impact. For example, one company decided to centralize its funds using Citi's tools to help ensure visibility. A second company chose to isolate its accounts from the outside world and cease transactions; with no access to electronic invoices, they were unable to validate payments and wanted to limit possible damage.

The first company was able to quickly triage and prioritize critical financial actions leveraging a printed payment schedule on hand and a clear set of principles (authorizing the treasurer to make on-the-spot decisions about fund movements, for example) to guide their actions. A third Citi client had made extensive preparations and was able to switch its entire operation to personal devices and paper within 20 minutes as the virus spread to its operations in many countries, leaving it with no network printers or communications.

What these reactions reveal is that while there is a tendency to see cyberattacks as a technological event, people and processes are critical to rapidly responding, containing and minimizing the impact. Seemingly mundane matters, such as having a printed list of phone contacts for contingency situations, are vital when all networks (and stored telephone numbers) are inaccessible; they can make the difference between resilience and catastrophe in the event of a cyberattack.

Planning – identifying general principles

It is impossible to accurately predict every potential cyberthreat. Therefore, an organization's preparation should be based on general principles and broad communications and governance guidelines along with potential response options that can be deployed in different ways depending on the severity of the cyber event.

One useful way to plan for cyber events is to consider the scale of possible compromise scenarios. For example, a small event may impact a limited number of desktop PCs; a medium-sized event may affect enterprise resource planning or treasury management systems; a "doomsday" event (of the type experienced as a result of Not-Petya or WannaCry) may put all PCs, networks and phones out of use.

Planning should identify critical functions and data, not just within the organization but also where there are vendor or supplier dependencies (including banks). Questions to be considered include:

- Who is empowered to make decisions?
- What are the priorities in terms of action?
- What alternative forms of communications should be used if there is no network or email?
- Who should be contacted at the bank or vendor?
- Should access to all bank services be restricted or should visibility be prioritized?
- Should clients or counterparties be contacted, and if so, by whom?

Treasury also needs to ensure that the right tools are in place and appropriate subject matter expertise is available including technology, legal and others as appropriate from inside and/or outside the organization. Planning efforts should be undertaken together with broader corporate efforts with treasurers highlighting the criticality of certain functions and systems so they can be prioritized appropriately.

Determining acceptable alternatives

A strategic contingency plan should identify alternative means of communication and interaction (with banks, for example) in the event of a cyberattack. Almost inevitably, an emergency situation is likely to require the use of non-standard equipment or software. Risks associated with an organization's using a personal laptop to access CitiDirect BE® or using thirdparty instant messaging software to communicate need to be balanced by the organization against an inability to access treasury workstations or use work telephones.

Treasury should consider whether its choice of alternative communication method meets regulatory guidelines for data management. The broader legal implications of how a company responds to a cyber-event should also be addressed. In the aftermath of a cyberattack, a company may be exposed to claims regarding their prioritization of various subsequent tasks, so therefore, a company should consider seeking legal guidance when devising their plan.

Citi's capabilities can help in many contingency scenarios by offering alternative options. For example, tools such as CitiDirect BE® are available via multiple platforms including desktop, mobile and tablet devices. Staff may need to be trained on how to use alternative platforms or software to help ensure effective operations should networks and other infrastructure fail following a cyberattack.

Recovering from crisis

A cyber event has many similarities with continuity of business planning for natural disasters or terrorism, including addressing how critical operations can be continued, the location of an alternative site, and how critical data is transferred.

However, because of the interconnectivity of cyber-related threats, backup infrastructure may need to be isolated from regular networks (although regularly updated). Clearly, such contingency capacity is costly: A company must determine its minimum critical infrastructure in order to help limit losses and damage to its business and invest accordingly. Furthermore, a cyberattack has additional risks such as potential fraud or stolen data, which can require additional expertise and considerations for a robust response plan.

Another important decision is prioritization of any replacement resources, such as PCs, in order to return to business as usual. Of course, it is advisable to establish and eliminate the root cause of the cyberthreat before bringing new systems online. Citi can help clients in an effort to resume business as usual as rapidly and safely as possible by managing overdraft positions to support FX and payment flows and removing of account restrictions once a risk assessment is successfully completed. Planning for an orderly transition back to business as usual can minimize impact of a cyber event and reduce the likelihood of potential further damage.

Developing a strategic contingency plan – best practices

A robust tested recovery plan is essential for Citi and its clients.

Plan

- Create and update recovery playbook
- Review possible threat/compromise scenarios
- Identify critical functions and data
- Include vendor/supplier dependencies (e.g. Citi)
- Ensure critical resources, expertise and skills are included
- Internal Communication and Training

Test

- Regular tests of recovery plan
- Simulations of compromised front and back-end systems
- Alternative payments/ Citi systems (e.g. CitiDirect BE Mobile, Manual Instructions)
- Communication protocols and expertise
- Personal knowledge of procedures

Recover

- Back-up infrastructure uploaded but isolated
- Off-line access to plan and response process
- Policies in place to ensure high continuity of business security
- Root cause investigation
- Insurance and reconstitution of normal operations

Response Process Flow

The following Cyber Response Planning Checklist has been developed to assist you in starting your contingency planning. (Please go to next page)

Cyber Response Planning Checklist (Sample Only)

1. Communication and Governance

☐ Critical internal partner contacts

Internal Partner	Name	Email	Phone
IT			
Legal			
Risk/Compliance			
PR			
Information Security			
Fraud Ops			

☐ Critical External partner contacts

External Partner	Name	Email	Phone	Website
Bank 1				
Bank 2				
Vendor 1				
Vendor 2				
Law Enforcement				
Regulator				

☐ Alternative contacts for core Treasury/Finance Team

Core Team	Email	Mobile	Preference
Senior Manager			
Business Manager			
Business Analyst			
Operations Lead			
Operations			
Controls, etc.			

☐ Primary contacts and Governance for Cyber Incident Response

Role	Name	Responsibility	Work Phone	Mobile	Email	Personal Email	Other
Treasury/Finance Head							
Senior Technology Manager							
Operations Head							
Controls/Fraud Manager							

2. System/Application Priority

	Core System and Infrastructure
1	
2	
3	
4	
5	

3. Transaction Priority

	Core System and Infrastructure
1	
2	
3	
4	
5	

4. Priority Market Positions

	Core System and Infrastructure
1	
2	
3	
4	
5	

Cyber Response Planning Checklist (Sample Only)

5. Cyber Readiness

- ☐ Ensure COB plan accounts for cyber incident, including doomsday scenarios
  - ☐ COB plan is tested regularly
  - ☐ COB site on a separate and independent network from main network
- ☐ Effective cyber defense with processes and policies to Protect, Detect and Respond
- ☐ Identify critical systems to run your business and outline minimum infrastructure needed to remain operational
- ☐ Centralize and empower control team with authority to make decisions during crisis
- ☐ Set up contingency payment methods
- ☐ Consider cyber insurance
- ☐ Review and familiarize with each bank's "Fraud Prevention Toolkit," if available
- ☐ Critical information back-up
  - ☐ Hard copy of all account numbers and banking relationships
  - ☐ Hard copies of all supplier relationships, invoices and payments processed
  - ☐ All phone numbers and email addresses of staff and relationship managers
  - ☐ Dual reconciliation on accounts, electronic statements and alternative source

6. Facing the Doomsday

- ☐ Risk assessment of compromised systems and scope of impact
- ☐ Invoke crisis plan depending on the situation
- ☐ Partially or completely shut down all systems: ERP (SAP), TMS (GTS), all applications, WiFi
- ☐ Consider cutting connectivity to 3rd parties
- ☐ Access to business reports (e.g. transactions, invoices)
- ☐ Visibility across client definitions
- ☐ Review payments in flight or pending
- ☐ Things you may request to your Bank:
  - ☐ Review outlier transactions, new beneficiaries, or payments to high risk countries and jurisdictions
  - ☐ Disable Host to Host connectivity
  - ☐ Apply account restrictions regionally or globally
  - ☐ Post Account Restrictions (Post No Credits, Post No Check, Post No Debits/ACH Block)
  - ☐ Service team partnership to manually release and process critical payments

7. Keeping up with business during crisis

- ☐ Prioritize transaction types that need to be executed urgently
- ☐ Suspend Target Balancing Sweeps (optional)
- ☐ Clear and decisive governance process
- ☐ External communication on any business delays
- ☐ Seek bank support for safe operation:
  - ☐ Reconciliation between ERP system and payments in flight or urgent payments for validation of beneficiary, amount, destination
  - ☐ Provide guidance or support for contingency options
  - ☐ Secure authentication method via personal smartphone
- ☐ Seek bank support in the event of fraud:
  - ☐ Provide cyber security intelligence
  - ☐ Dedicated team to investigate fraud
  - ☐ Invoke bank fraud process
  - ☐ Initiate a recall
- ☐ Other considerations actions in the event of fraud:
  - ☐ Temporary block on payments
  - ☐ Notify law enforcement authorities

8. Recovering

- ☐ Ensure most important payments are prioritized
- ☐ Assurance framework to turn payment systems back on
- ☐ Prioritize which systems to return or turn on first
- ☐ Consider lifting imposed restrictions on accounts and PND, using a phased approach
- ☐ External communication on the cyber incident impact
- ☐ Seek bank support to:
  - ☐ Resume Business As Usual across regions and global footprint
  - ☐ Manage overdraft positions to support FX and payment flows
  - ☐ Account reconciliation for reporting purposes

1673124 03/18

Treasury and Trade Solutions
transactionservices.citi.com

GRA29796 09/2018