# 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 | |

Treasury and Trade Solutions

# 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