Contact via 312-880-7798, info@lauer-financial.com, or www.lauer-financial.com

LAUER FINANCIAL LLC
CYBERSECURITY INCIDENT RESPONSE PLAN

OVERVIEW

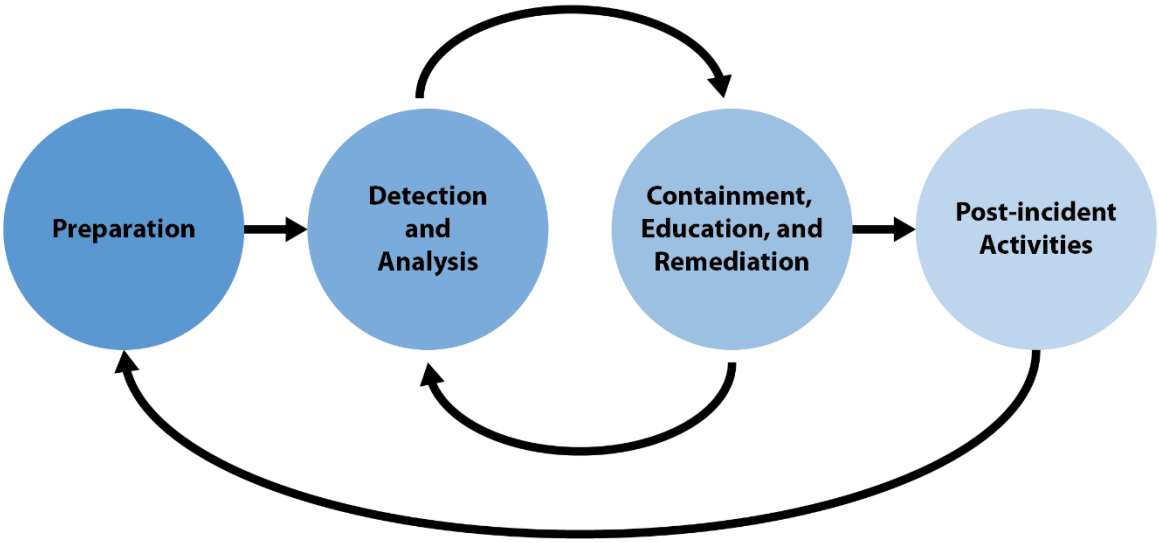
This Cybersecurity Incident Response Plan ("Plan") defines what constitutes a cybersecurity incident and outlines the incident response phases. The Plan explains how Lauer Financial LLC (the "firm") will handle an event including sharing of information with appropriate parties, assessing the event, and properly working to minimize exposure or damage from the event.

The Plan also details how an event should be documented and how to preserve information if necessary. The Plan defines areas of responsibility and establishes procedures for handling various cybersecurity incidents.

PURPOSE OF THIS PLAN

- Keep management informed
- Prevent future incidents
- Explain the role of the Cybersecurity Threat Intelligence (CTI) team
- Establish the Cybersecurity Incident Response team (CSIRT), which will:
  - Verify an incident has occurred
  - Maintain or restore business operations
  - Reduce impact of any incidents
  - Notify necessary parties
  - Determine attack vectors

INCIDENT RESPONSE LIFE CYCLE



CYBERSECURITY INCIDENT PREPARATION

CTI TEAM

The CTI team's responsibility is to assess and defend against cyber threats. This team is responsible for ensuring adequate systems and processes are in place for detecting and analyzing the following threat types:

- Loss of customer or employee personally identifiable information (PII)
- Data corruption
- Distributed denial of service (DDoS) attacks
- Network intrusions
- Customer account intrusions
- Virus or malware infection
- Theft of physical information technology (IT) asset

ESTABLISH CSIRT

The CSIRT is responsible for receiving, reviewing, and responding to cybersecurity incident reports and activity. This is an ad-hoc team that is called together during an ongoing incident or to respond to an incident when the need arises.

INCIDENT DETECTION AND ANALYSIS

Steps involved in detecting and analyzing a particular incident relies on an in-depth strategy to identify incident types and start containment, eradication, and remediation depending on severity of the incident. The CTI team is responsible for initial classification of incidents and following the action steps noted below.

Other steps may be taken as appropriate or required, but initial guidelines are set forth below:

1. **Alert of Malware Activity**
    - Run anti-virus and malware scans to determine if the machine is infected
    - If activity is confirmed, record as an incident
    - If it is a low threat level, such as a Potentially Unwanted Program (PUP), attempt to remove the software
    - If it is a higher threat level, a low level threat that is unable to be removed, or the threat level cannot be determined, the machine should be removed from the network and reimaged
    - If the malware is a Trojan or has any form of call back, network passwords should be reset

2. **Notice of Phishing Emails**
    - Any destinations of links in the email should be blocked
    - Review system to check how many copies of the email have been received
    - If a link is clicked by a user, record the incident and follow the Malware Activity Response steps in this document
    - Work with technology support to have the email removed from all system mailboxes
    - Communicate to users if the issue is widespread or uses a sophisticated approach
    - Record the incident

3. **Lost or Stolen Keycards**
    - Deactivate keycard
    - Record the incident

4. **Lost or stolen Equipment** – Includes all devices: iPad or other tablet, laptop, mobile phone, hard drive, etc.
    - Record the incident.
    - Determine if any PII has been put at risk
    - If PII is at risk, notify the CSIRT
    - Deactivate any account specifically linked to the equipment (e.g., RSA token)
    - If theft, report the theft to insurance carrier and/or law enforcement as appropriate

5. **Internal Unauthorized Access to a Resource**
   Internal unauthorized access: Employee or business asset accessed a resource without authorization
    - Record the incident
    - Determine if any PII has been put at risk
    - If PII is at risk, notify the CSIRT. Otherwise, notify relevant stakeholders.
    - Determine the cause of the incident and remediate to prevent future instances

6. **External Unauthorized Access to a Resource**
   External unauthorized access: An external threat actor (e.g., a hacker)
    - Record the incident
    - Determine if there is a threat to PII or network integrity
    - If it is determined there is a threat, notify the CSIRT
    - Determine the cause of the incident and remediate to prevent future instances.

7. **Failure of Physical Security**
    - Record the incident
    - Determine if there was a threat to employee safety and/or PII
    - Notify relevant stakeholders
    - Notify insurance carrier and/or law enforcement as appropriate
    - Determine the cause of the incident and remediate to prevent future instances

8. **Intrusion Prevention System (IPS) Notifications**
    - If it is a High Severity notification or if the alert is confirmed, record the incident
    - Determine if there is a threat to PII or network integrity
    - If it is determined there is a threat, notify the CSIRT
    - Determine the cause of the incident and remediate to prevent future instances

9. **Shared Individual Network Credentials**
    - Record the incident
    - Any shared passwords are to be reset
    - Notify relevant stakeholders and supervisors to remediate and prevent future instances

NOTIFICATION, ESCALATION, AND DECLARATION

During an incident response, the CTI team will communicate with the CSIRT as appropriate. The Incident Lead or designee will establish a secure conference method and meeting location as necessary.

- If PII, systems, or credentials could be compromised, notify Cambridge Information Security Team (security@cir2.com) for further assistance and reporting.

- If the firm is registered in the state of New York, the CSIRT shall notify the New York Superintendent of Financial Services as promptly as possible, but in no event later than 72 hours from a determination that a cybersecurity event has occurred that is either of the following:

    1. Cybersecurity events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body; or
    2. Cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity

It will be the sole discretion of the CSIRT to invoke the Business Continuity Plan (BCP).

POST INCIDENT

All incidents reported to the CSIRT will have a post-mortem analysis performed by its members to determine ways to prevent future occurrences of the incident and improve the overall process. This meeting should occur as soon after the incident as reasonably possible.