Geldi Omeri
ITMS-588

Incident Response Policy

Purpose

The purpose of this document is to define Very Safe Bank's Incident Response Program. The program contains the overall plan for preparing and responding to physical and electronic information security incidents in a quick and decisive manner in order to limit the impact of an adverse event on the bank's customers and information resources. It also defines the roles and responsibilities of participants, characterization of incidents, and reporting requirements. This policy also defines the methods and measures to be taken to insure timely corrections of any damage caused by an incident and to provide for effective investigation and follow-up actions to reduce the likelihood of an incident occurring or reoccurring.

Scope

This plan applies to the physical locations of Very Safe Bank, the physical and electronic information systems operated by them, and any bank information systems that are operated by third party service providers or agents on Very Safe Bank's behalf. All employees, including temporary, part-time, and contract are covered by the policy.

Policy

General Requirements

The following requirements are established through this policy:

- An Incident Response Team will be implemented within Very Safe Bank. Through this policy's approval, the IRT is granted the authority to act and make decisions as necessary to respond appropriately to an incident.
- The IRT member's have defined roles and responsibilities, which are outline below. These responsibilities supersede normal duties in the event of a security incident.
- An event classification system will be used to define incidents by their level of severity and will be used to mange incident response process and provide guidance for escalation.

- Whenever a security incident is suspected or confirmed, all parties covered by this policy are expected to follow appropriate procedures and instructions given by the IRT.

Incident Identification & Definition

Event - An event is an exception to the normal operation of infrastructure, systems, or services. Events are not inherently incidents.

Incident – Any irregular or adverse event that involves the availability, integrity, or confidentiality of the bank's systems or networks. They can be either physical or electronic in nature.

Incidents can include:

- Malware/Viruses
- Ransomware
- Phishing
- Unauthorized Electronic Access
- Breach of Information
- Unauthorized Physical Access
- Denial of Service/Unwanted Disruptions
- Identity Theft of Bank Customer
- Unauthorized Debit or Credit Card Activity
- Loss or Destruction of Physical Files

IR Team

Through this policy's approval, the Incident Response Team has been authorized to take appropriate actions as outlined in this document. The members of the IRT are listed below.

<u>IRT Members:</u>

- Chief Information Officer (IRT Leader)
- Chief Financial Officer
- IT Staff
- Senior Operations Officer
- Loan Operations Officer
- Senior Risk Officer
- Corporate Marketing Manager

- Human Resources Manager
- Corporate Council

Incident Identification, Classification, and Escalation

Once a suspected incident has been detected, it is the responsibility of the respective individual to report it, as outlined below. The nature and severity of the incident will determine the response strategy to be applied. Levels of severity are defined below. The decision to classify an incident according to these definitions falls onto the CIO (the IRT Leader). The CIO is also responsible for escalating or downgrading the severity of an incident based on any changes in circumstances. Severity levels are as follows:

High – An incident where the impact is catastrophic. The incident can cause significant damage, corruption, or loss of confidential, critical, and/or strategic bank and customer information. It can result in potential damage and liability to the bank and its reputation. It may degrade significantly degrade customer confidence in the bank and its services. Examples include computer intrusions, compromise of critical information, shutdown of all network services.

Medium – An incident where the impact is significant. The incident can cause damage, corruption, or loss of replaceable information without compromise or may have a moderate impact on bank's operations or reputation. Examples include misuse or abuse of authorized access, accidental intrusion, confined malware infection, system crashes, or unusual system performance or behavior.

Low – An incident where the impact minimal. The incident can cause inconveniences, aggravation, minor costs, unintentional actions at the user or administrator level, unintentional or minor loss of recoverable information, and there would be little impact on the bank's operations or reputation. Examples include sharing of passwords, policy or procedural violations, e-mail SPAM, isolated virus infection.

Incident Reporting

All Very Safe Bank employees, contractors, and colleagues are responsible for helping to ensure the security of the information systems that they use and operate. This extends to reporting any confirmed or suspected security problems in a timely manner. Upon a report being submitted, the IRT will be activated to further investigate and respond to the incident.

Incident Response and Escalation

The response process consists of four core phases:

- Identification – The incident is recognized/suspected, reported, and confirmed
- Assessment – The incident is evaluated, and an initial severity rating is assigned
- Response – An appropriate strategy is determined, executed, and revised as needed
- Follow-up – Damage is corrected, vulnerabilities are identified and rectified, and summary reports are prepared

The decision to escalate is a made by the CIO and the IRT team based on the changing circumstances of the occurring incident. The escalation process will be initiated to involve other appropriate resources as the incident increases in scope and impact.

Recovery

The CIO is responsible for recovery and documentation of all recovery activities during the incident.

Recovery efforts for incidents will involve the restoration of affected system to their normal operations. This is dependent upon the nature of the incident and its impact. This may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, and updating passwords.

Internal and External Communication

To ensure that information is disseminated quickly and consistently, specific responsibilities for communications inside and outside the bank fall on the CIO and are outlined below.

- The CIO is responsible for notifying the bank president and IRT members and initiating the appropriate incident management action.
- The CIO is responsible for reporting the incident to appropriate local, state, or federal law officials as required by applicable regulations.
- The CIO is responsible for coordinating communications with outside organizations (law enforcement, insurance companies, regulatory agencies, etc.)
- The CIO will determine if a widespread bank communication is required, the content of the communication, and how to best disseminate the communication.

- The CEO will serve as the spokesperson for Very Safe Bank for communication with the media and public.

Collection/Protection of Information and Reporting

The CIO is responsible for determining the evidence to be gathered as part of the incident investigation. The bank must take precautions to ensure that evidence is always accounted for the chain of custody for evidence is fully documented. Depending on the nature of the incident, a suspicious activity report may need to be filed with law enforcement and regulators.

Lessons Learned

The CIO is responsible for initiating, completing, and documenting the incident investigation with assistance from the IRT. A report must be prepared to be submitted to the Executive Committee, which includes the following information:

- The Incident Type – this may include denial of service attacks, vandalism, unauthorized access, widespread malware or ransomware attacks, identity theft, etc.
- The Response Strategy – includes all actions that were taken by all parties in managing the incident.
- How the Incident Occurred – including weakness in the process, vulnerabilities in systems and physical controls.
- Recommendations for Prevention of Similar Incidents Arising in the Future