PathStone

Connecting You to Opportunities

PATHSTONE CORPORATION CYBER INCIDENT RESPONSE PLAN

2022

Purpose

This document describes the PathStone overall plan for preparing and responding to electronic information security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, reporting requirements, and escalation processes.

Relationship to other documents

This document was created to work in conjunction with the "PathStone Disaster Recovery and Business Continuity Plan". When appropriate, some information contained in that document and its appendices is referenced here.

Definitions

Incident

An incident is an event that, as assessed by the staff, violates the policies of PathStone as related to Information Security, Physical Security, or Acceptable Use.

Incidents can include:

Malware/viruses/Trojans- especially those affecting servers or cloud systems

Ransomware

Phishing- if widespread or results in possible malware or critical information leak

Unauthorized electronic access

Breach of information

Unusual, unexplained or repeated loss of connectivity

Unauthorized physical access to IT/Server areas

Loss or destruction of physical files, etc.

Communication

**See DR Plan Appendix C2- "IT_Finance_HR Critical Vendor List"

CIO

CEO, General Counsel, other internal stake-holders

IT Security Vendors

Cyber Insurance Carrier

Brown and Brown Insurance

Law Enforcement

Banks or other Financial Institutions

PathStone Employees

Escalation

Incidents will be escalated as needed to communicate to stakeholders (see Communication). Also, escalation may be appropriate as per guidance from cyber carrier, law enforcement, General Counsel, or Exec. Staff. In general, the CIO should be notified initially, and may decide on further escalation as needed. Most likely escalation will include one or more of PathStone's technology vendors.

If data recovery or use of DR Site is deemed necessary- the necessary steps are outlined in the "PathStone Disaster Recovery and Business Continuity Plan".

Incident Reporting

Incidents should be reported to the CIO directly, as well as to the PathStone IT Helpdesk: helpdesk@pathstone.org. The CIO may decide on further reporting, including CEO and Exec. Staff, Brown and Brown Insurance, and Cyber Insurance Carrier. Other regulatory agencies may be notified if appropriate, as well as funders or other stakeholders.

If there has been a breach of PathStone's data, the CIO and General Counsel will work with Executive Staff to determine what disclosures and reporting of such breach must be made.

Evidence Preservation

If there is evidence of malicious activity it is important to maintain data, emails, computer or server image backups, and other data. This data may be needed by forensic teams as well as regulatory agencies. The need to return to normal working state as soon as possible must be balanced with the need to keep forensic information intact.

Post-Incident Activity

Analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" into future response activities and training.

Documentation. It is important to fully document:

- Systems affected
- All actions taken
- External and relevant internal communications
- Any changes made during the incident
- Data loss (if any)

Lessons learned. Evaluate how current systems performed and plan for any needed improvements

- What changes should be made to prevent similar future incidents
- Improvements to security software or procedures
- External vendor partnerships
- Cyber policy changes
- How well did backups and data retention polices perform

If a Breach has occurred it may be necessary to communicate to affected parties, regulatory agencies etc.

Legal action if deemed appropriate

Review entire incident with management and internal stakeholders