

Fraud Report

Fraud #: F-20-102

Submission Date: 03/10/2020

Entity: Bainbridge Island Metropolitan Park and Recreation District

Dashboard

Short Description: 2 hard drives hacked

Investigation Status: Closed

Assigned Team: Port Orchard

Assigned PM:

Assignment Notes:

Detection Method: Entity Management

Entity: 1685

Total Budget: 4

Team Budget: 4

Audit Number: 57636

Audit Documentation: Database Only

TM Project Code:

Ok to release/bill time: No

Primary Loss Type: Cyber Concerns

Loss Type Notes or Sub Category: wiped data off harddrive

Cyber Loss Category: Cyberattack

Cyber Cause: --

This case contains sensitive information: No

Which tab or attachment contains sensitive information?

Results: No Action - consider risk on next audit

Closed Date: 05/12/2020

Inactivate: No

Inactive Notes:

Contact

Created By:

Name: Amy Swenson

Title: Finance/HR Director

Phone: 2068422306

Email: amy@biparks.org

Assignment Notes:

Paw and Plan

Loss Notification Date: 03/10/2020

PAW Assignment Date:

Initial Contact with Entity Date:

Assessment Completion Date:

Reviewing Team: Cybersecurity Audit

Team Review Date:

Fraud Team Review Date:

Please describe, if we did not meet 5 and 10 day requirements:

Action/Next Step:

Outcome

Exit conference date:

Exit conference attendees:

Misappropriation assigned amount:

Name and title of responsible party:

Misappropriation unassigned amount:

Questionable amount:

Misappropriation recovery amount:

Loss Amount:

Cyber recovery Amount:

Final audit cost:

Audit report number:

Audit report issue date:

Other case # s reported with this one:

Restitution

SAO Approval Date:

SAO Approval Initials:

AG Approval Date:

SAO Approval Initials:

Amount Approved:

Point of Contact:

Contacted PA Date:

Post audit PA/LE/FBI contact notes:

Activity Log

Date	Entry
03/11/2020	Sent to Peg for IT security risk review. (gillisj)

03/11/2020	Fraud updated by gillisj
03/11/2020	Fraud updated by gillisj
03/11/2020	Fraud updated by gillisj
03/12/2020	Fraud updated by gillisj
03/12/2020	Fraud updated by gillisj
03/12/2020	Fraud updated by gillisj
04/01/2020	PAW exported
05/12/2020	Attachment added
05/12/2020	The entity reports there was no impact to the financial records. We will close case. (sullivans)
05/12/2020	Fraud updated by sullivans
05/12/2020	Fraud closed by sullivans
07/28/2022	'Total Budget' field updated from '' to '4', 'Loss Type Notes or Sub Category' field updated, 'Cyber Loss Category' field updated from '--' to 'Cyberattack', 'Team Budget' field updated from '' to '4' by pritchab
11/22/2024	'Reviewing Team' field updated from '213' to '260' by pritchab
11/22/2024	'Assigned Team' field updated from 'Cybersecurity Audit' to 'Port Orchard' by pritchab

Initial Loss Report

Department/area of concern: Computer Hacking

What is the suspected loss or illegal activity? 0

Start: 02/29/2020

End: 02/29/2020

What type of issue are you reporting? Cyber Concerns

What type of cyber concern are you reporting? Cyberattack

What was the cause of initial attack vector for the cyber loss? --

Please describe the type of issue:

Please describe the amount of loss:

Please describe the suspected loss of illegal activity: SUBMITTED DESCRIPTION: Our hard drive (2) were hacked and all the data plus our back up data was wiped clean. We are able to rebuild from a data cloud back up but we have been without an accounting system for two weeks as the system is brought back.

How was the suspected loss or activity detected? We were unable to log in, connect to the internet. Our IT people checked and found the servers compromised.

Is an investigation in progress? Yes

If an investigation by management, law enforcement or others underway, who is in charge of this

investigation? We have hired a forensic IT person (through our insurance - Enduris) to try and find out what happened.

What actions have you taken to date, if any? restoring and hiring a forensic person to look at the computer. Also hired an attorney to help us figure out reporting requirements.

Are there any dedications of employee involvment? cannot tell.

Name and/or title of employee that have been involved in (responsible for) the loss.

Is this person still employed by the agency? No

Describe the employee's job responsibilities and areas or functions the employee has/had access to:

Have any restitution agreements been signed? No

Has a police report been filed? No

Do you have a copy? No

Who at the entity is aware this concern is being reported?

Fraud Investigation Preliminary Assessment Worksheet

Fraud Case Number	F-20-102
Client	Bainbridge Island Metropolitan Park and Recreation District
Fraud Specialist	Nick Benfield (benfieldn@sao.wa.gov)
Loss Notification Date	3/10/2020
Initial Contact with Entity Date	3/23/2020
Assessment Completion Date	4/6/2020
Team Review Name	IT Audit
Team Review Date	4/9/2020 Erin Laska
Fraud Manager Review Date	4/10/2020
Action/Next Step	Close case with e-mail or phone call to entity

The preliminary assessment worksheet summarizes the pre-planning information needed for the triage meeting. An assessment does not need to be completed on loss reports that do not require action per policy (losses resulting from breaking and entering or property vandalism normally handled by a law enforcement agency or by the entity, or other losses such as reasonable cash-receipting overages/shortages, reasonable inventory shortages or other de minimis losses).

Reported Loss Information		
1	Description of suspected loss or illegal activity	SUBMITTED DESCRIPTION: Our hard drive (2) were hacked and all the data plus our back up data was wiped clean. We are able to rebuild from a data cloud back up but we have been without an accounting system for two weeks as the system is brought back.
2	How loss was detected and reported	We were unable to log in, connect to the internet. Our IT people checked and found the servers compromised.
3	Type of loss (e.g. cash receipts, disbursements, payroll)	Cyber Concerns
4	Reported amount of loss	\$0
Information from EIS and Audit Manager		
5	Entity liaison name	Amy Swenson
6	Entity liaison title	Finance/HR Director
7	Entity liaison phone number	206.842.2306
8	<input type="checkbox"/> Related audit exceptions in EIS	
9	If yes, what was level of reporting (exit item, mgmt letter, or finding)?	Nothing related
10	If applicable, summarize your review of TeamMate audit work related to area of reported loss.	N/A
11	Summarize any audit manager's concerns about client and reported loss.	No concerns

12	Normal audit scope and cycle for client?	Accountability Cycle: 2-year; Financial Cycle: 2-year; Single Audit Cycle: None
13	Accountability audit budget?	90.0
14	Is the audit team currently conducting an audit? If yes, what is the status and scope (financial, single or accountability)? If not, when is the audit scheduled to start?	Audit will be completed Fall 2020
15	Any other relevant information?	N/A
Information from Client		
16	<input type="checkbox"/> The individual suspected in the loss has access to other accounting/financial systems or bank accounts.	
17	If yes, list those systems and accounts.	Click here to enter text.
18	<input type="checkbox"/> The client has properly secured records or evidence related to the loss	
19	<input type="checkbox"/> Potential for additional loss or other areas of risk for loss - "What Else"	
20	If yes, summarize.	N/A
21	When was the individual hired by the client?	Month Click here to enter text. Year Click here to enter text.
22	<input type="checkbox"/> The individual has been in different job positions with the client and there have been employment history issues	
23	If yes, list the position, time-period and issues.	Click here to enter text.
24	What is the current employment status of the individual (e.g. administrative leave on XX date)?	Click here to enter text.
25	<input checked="" type="checkbox"/> The client conducted an investigation	
26	If yes, summarize results.	Click here to enter text.
27	<input type="checkbox"/> A police report has been filed	
28	<input type="checkbox"/> Law enforcement is investigating	
29	<input checked="" type="checkbox"/> Another outside party (FBI, OIG, LEAs or other investigator) is conducting an investigation. FBI notified	
30	<input type="checkbox"/> The client has established a time table of events that occurred up to the reported loss. (If not, recommend they document the key events.)	
31	<input type="checkbox"/> There is a fixed responsibility	
32	Who within the client has been notified of the loss (commissioners, board, elected officials, etc.)?	Entire organization was informed
33	<input type="checkbox"/> The County Prosecutor has been notified	
34	Has legal counsel has been obtained by the individual?	Unknown
35	<input type="checkbox"/> The client has entered into restitution agreements	
36	Any other relevant information?	On the weekend of the February 23 rd encryption was used to render the entity's servers inoperable, however no ransom was given. The Entity Recovered from backups that were stored in AWS glacier (cloud backup). There was a three week disruption in operations as servers and services were reconstituted. The last service re-established was the financial system. During the outage employees were issued paper checks for one pay period.

		<p>The Entity's Insurance Company was notified and hired a forensics experts and a privacy lawyer to assist in the event. Results from the forensics investigation should be presented to the Entity in the coming weeks. The Entity also notified the FBI, Fusion Center, however did not file a case with local authorities. All employees were also informed of the event.</p> <p>The local contractor managing the IT infrastructure informed us that the hard drives on the SAN were encrypted and set back to factory defaults. He then theorized that remote desktop was likely the initial vector of infiltration. Completion of the forensic analysis should be more conclusive.</p> <p>The entity reports there was no impact to the financial records because they backed up to the cloud on the Friday afternoon and the attack happened on the weekend. For three weeks they kept paper records and those were added after access came back.</p> <p>No suggestions were made to the entity to prevent future issues because the entity has a forensics expert working with them.</p>
--	--	---