Cory Thomas

4/17/2019

Course Project

As Chief Information Assurance Officer of QIR my investigation has been completed, The alleged contact between QIR and IBM officials. I have conducted a forensic analysis on the laptop and cell phone of a high-ranking QIR employee. During the investigation I have found a text between Lucas Green and Bryan Zoom. Brayan Zoom is a current IBM employee.

The text was about a confirmation for a lunch meeting on 2/15/2019 and the phone number was labeled “Lucas Green “, in the contact list. The laptop had several email communications about meetings and payment for "consulting services" between the official and BryanZoom@gmail.com. There were several deleted zip files of classified material that web logs show were uploaded to a file sharing site. It is not clear if they were downloaded by anyone. The file was deleted but I was about to recover parts of the file that was corrupted. With the investigation that was conducted I recommend that employee Lucas Green is to be terminated at once and to be charged with theft and for violating the privacy act. Also I have provide and updated the new policies that will prevent this from happening again in the future to come.

REPORT OF PRIVACY ANALYSIS

MEMORANDUM FOR: FBI

Investigator THOMAS

NORFOLK, USA 01234

***SUBJECT*:** Forensic Analysis Report

Subject: Lucas, Green

Case Number: 012345

Status: PENDING

Actions on

1. Legal authority was established by a search warrant obtained specifically for the examination of the computer and cell phone in a laboratory setting.
2. Chain of custody was properly documented on the appropriate departmental forms.
3. Evidence intake was completed.

a. The evidence was marked and photographed.

b. A file was created, and the case information was entered into the laboratory database.

c. The computer and cell phone were stored in the laboratory's property room.

Imaging

1. The notebook computer was examined and photographed.
2. The hardware was examined and documented.
3. The notebook computer was powered off without making any changes to the BIOS
4. EnCase was used to create an evidence file containing the image of the notebook computer's hard drive.

5. The notebook computer was connected to a laboratory computer through a null modem cable, which connected to the computers' parallel ports.
6. The notebook computer was booted to the DOS prompt with a controlled boot disk and EnCase® was started in server mode.
7. The laboratory computer, equipped with a magneto-optical drive for file storage, was booted to the DOS prompt with a controlled boot disk. EnCase® was started in server mode and evidence files for the notebook computer were acquired and written to magneto-optical disks.
8. When the imaging process was completed, the computers were powered off.
9. The notebook computer was returned to the laboratory property room.
10. The magneto-optical disks containing the EnCase® evidence files were write-protected and entered into evidence
11. Cell phone was examined and photographed.
12. The device was examined and documented.

Summary of Findings:

- Cell Phone – communication to and from Bryan Zoom in the contact list. 2/15/2019
- laptop - communications to and from Bryanzeee@gmail.com
- laptop - several deleted zip files of classified material.

Items Analyzed:

TAG NUMBER:	**ITEM DESCRIPTION:**
012345	One Generic laptop, Serial # 123456789
012346	One Generic cellphone, Serial #2382723

Details of Findings:

■ Findings in this paragraph related to the Generic Hard Drive, Model ABCDE, Serial # 3456ABCD, recovered from Tag Number 012345, One Generic laptop, Serial # 123456789.

1) several email communications about meetings and payment for "consulting services" between the official and Bryanzeee@gmail.com

2) several deleted zip files of classified material that web logs show were uploaded to a file sharing site. It is not clear if they were downloaded by anyone.

■ Findings in this paragraph related to the Generic Cellphone, Model EDWDS, Serial # 2727ASD, recovered from Tag Number 012346, One Generic cellphone, Serial #2382723.

1) text confirming a lunch meeting on 2/15/2019

2) phone number was labeled "Bryan Zoom" in the contact list.

Glossary:

Shortcut File: A file created that links to another file.

Items Provided: In addition to this hard copy report, one compact disk (CD) was submitted with an electronic copy of this report. The report on CD contains hyperlinks to the above-mentioned files and directories.

Result: Personnel has provided proof of espionage, should be detained and prosecuted.

CORY THOMAS Released by_____

Computer Forensic Examiner

Security Response Plan Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to* QIRLLC@email.gov .

Last Update Status: *Updated June 2019*

1 Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

2 Purpose

The purpose of this policy is to establish the requirement that all business units supported by the Infosec team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

3 Scope

This policy applies any established and defined business unity or entity within the QIR

4 Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the Infosec Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the QIR in the development and maintenance of a Security Response Plan.

4.1Service or Product Description
The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2 Contact Information
The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3 Triage
The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4 Identified Mitigations and Testing
The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5 Mitigation and Remediation Timelines
The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5 Policy Compliance

5.1 Compliance Measurement
Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2 Exceptions

Any exception to this policy must be approved by the Infosec Team in advance and have a written record.

5.3 Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP

6 Related Standards, Policies and Processes – none

Revision History

Date of Change	Responsible	Summary of Change
June 2019	SANS Policy Team	Updated and converted to new format.

Data Breach Response Policy

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

QIR Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how QIR established culture of openness, trust and integrity should respond to such activity. QIR Information Security is committed to protecting QIR 's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1Background

This policy mandates that any individual who suspects that a theft, breach or exposure of QIR Protected data or QIR Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@ QIR org, by calling 555-1212, or through the use of the help desk reporting web page at http://QIR This e-mail address, phone number, and web page are monitored by the QIR Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of QIR members. Any agreements with vendors will contain language similar that protects the fund.

Policy Confirmed theft, data breach or exposure of QIR Protected data or QIR Sensitive data

As soon as a theft, data breach or exposure containing QIR data or QIR Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of QIR data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by QIR cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with QIR communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the QIR community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any QIR Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of QIR community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the QIR community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

4.0 Enforcement

Any QIR personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

5.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity) and can be linked to a specific individual.
Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered
Protected data - See PII and PHI
Information Resource - The data and information assets of an organization, department or unit.
Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

Revision History

Version	Date of Revision	Author	Description of Changes
1.0	August 17, 2019	QIR, LLC	Initial version

Work Cited Page

Information Security Policy Templates.” ***SANS*****,** **www.sans.org/security-resources/policies/general#security-response-plan-policy**

Guide to NIST: National Institute of Standards and Technology**. U.S. Dept. of Commerce, Technology Administration, 1998**