Penetration Test Preparation Report for Alexander Rocco Corporation

Prepared by: Stuart Howard

Date: 18 Jan 2024

1. Introduction:

Alexander Rocco Corporation has engaged our computer consulting company to perform a penetration test on its computer network. The objective is to assess the security of the network infrastructure, understand the network topology, and identify any vulnerabilities that may pose a risk to the company. Claudia Mae, the vice president, is our primary contact, and the testing will be conducted without the involvement of IT staff or employees to maintain the integrity of the assessment.

2. Legal and Regulatory Compliance:

Before commencing the penetration tests, ensuring compliance with relevant laws and regulations is essential. In this context, we have researched the laws applicable to the state of Hawaii and identified the following:

State Laws:

§708-890 Definitions. As used in this part, unless the context otherwise requires:

"Access" means to gain entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
"Computer" means any electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes all computer equipment connected or related to such a device in a computer system or computer network, but shall not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

"Computer equipment" means any equipment or devices, including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.
"Computer network" means two or more computers or computer systems, interconnected by communication lines, including microwave, electronic, or any other form of communication.

"Computer program" or "software" means a set of computer-readable instructions or statements and related data that, when executed by a computer system, causes the computer system or the computer network to which it is connected to perform computer services.

"Computer services" includes but is not limited to the use of a computer system, computer network, computer program, data prepared for computer use, and data contained within a computer system or computer network.

"Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

"Critical infrastructure" means publicly or privately owned or operated systems or assets vital to the defense, security, economic security, public health or safety, or any combination thereof, of the State or nation. "Critical infrastructure" includes:

(1) Gas and oil production, storage, and delivery systems;

(2) Water supply systems;

(3) Telecommunications networks;

(4) Electrical power delivery systems;

(5) Finance and banking systems;

(6) Emergency services, such as medical, police, fire, and rescue services;

(7) Transportation systems and services, such as highways, mass transit, airlines, and airports; and

(8) Government operations that provide essential services to the public.

"Damage" means any impairment to the integrity or availability of data, a program, a system, a network, or computer services.

"Data" means information, facts, concepts, software, or instructions prepared for use in a computer, computer system, or computer network.

"Obtain information" includes but is not limited to mere observation of the data.

"Property" includes financial instruments, data, computer software, computer programs, documents associated with computer systems, money, computer services, or anything else of value.

"Rule of court" means any rule adopted by the supreme court of this State, the Federal Rules of Civil Procedure, or the Federal Rules of Criminal Procedure.

"Statute" means any statute of this State or the federal government.

"Without authorization" means without the permission of or in excess of the permission of an owner, lessor, or rightful user or someone licensed or privileged by an owner, lessor, or rightful user to grant the permission. [L 1992, c 225, pt of §2; am L 2001, c 33, §4; am L 2003, c 3, §17; am L 2014, c 213,

§708-891 Computer fraud in the first degree. (1) A person commits the offense of computer fraud in the first degree if the person knowingly accesses a computer, computer system, or computer network with the intent to commit the offense of theft in the first degree.

(2) Computer fraud in the first degree is a class A felony. [L 2001, c 33, pt of §1; am L 2012, c 293, §2]

§708-891.5 Computer fraud in the second degree. (1) A person commits the offense of computer fraud in the second degree if the person knowingly accesses a computer, computer system, or computer network with the intent to commit the offense of theft in the second degree.

(2) Computer fraud in the second degree is a class B felony. [L 2001, c 33, pt of §1; am L 2012, c 293, §3]

[§708-891.6] Computer fraud in the third degree. (1) A person commits the offense of computer fraud in the third degree if the person knowingly accesses a computer, computer system, or computer network with the intent to commit the offense of theft in the third or fourth degree.

(2) Computer fraud in the third degree is a class C felony. [L 2012, c 293, §1]

§708-892 Computer damage in the first degree. (1) A person commits the offense of computer damage in the first degree if the person intentionally causes or attempts to cause damage to a computer, computer system, or computer network that manages or controls any critical infrastructure and the damage results in, or in the case of an attempt to cause damage would have resulted in if completed, the substantial impairment of:

(a) The operation of the computer, computer system, or computer network; or

(b) The critical infrastructure managed or controlled by the computer, computer system, or computer network.

(2) Computer damage in the first degree is a class A felony. [L 2001, c 33, pt of §1; am L 2014, c 213, §3]

§708-892.5 Computer damage in the second degree. (1) A person commits the offense of computer damage in the second degree if:

(a) The person knowingly causes the transmission of a program, information, code, or command, and thereby knowingly causes unauthorized damage to a computer, computer system, or computer network; or

(b) The person intentionally accesses a computer, computer system, or computer network without authorization and thereby knowingly causes damage.

(2) As used in this section, "damage" means:

(a) A loss aggregating at least $5,000 in value, including the costs associated with diagnosis, repair, replacement, or remediation, during any one-year period to one or more individuals;

(b) The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; or

(c) Impairment or disruption of government operations.

(3) Computer damage in the second degree is a class B felony. [L 2001, c 33, pt of §1; am L 2014, c 213, §4]

[§708-892.6] Computer damage in the third degree. (1) A person commits the offense of computer damage in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby recklessly causes damage.

(2) Computer damage in the third degree is a class C felony. [L 2014, c 213, §1]

§708-893 Use of a computer in the commission of a separate crime. (1) A person commits the offense of use of a computer in the commission of a separate crime if the person knowingly uses a computer to identify, select, solicit, persuade, coerce, entice, induce, procure, pursue, surveil, contact, harass, annoy, or alarm the victim or intended victim of the following offenses:

(a) Section 707-726, relating to custodial interference in the first degree;

(b) Section 707-727, relating to custodial interference in the second degree;

(c) Section 707-731, relating to sexual assault in the second degree;

(d) Section 707-732, relating to sexual assault in the third degree;

(e) Section 707-733, relating to sexual assault in the fourth degree;

(f) Section 707-751, relating to promoting child abuse in the second degree;

(g) Section 711-1106, relating to harassment;

(h) Section 711-1106.4, relating to aggravated harassment by stalking;

(i) Section 711-1106.5, relating to harassment by stalking; or

(j) Section 712-1215, relating to promoting pornography for minors.

(2) Use of a computer in the commission of a separate crime is an offense one class or grade, as the case may be, greater than the offense facilitated. Notwithstanding any other law to the contrary, a conviction under this section shall not merge with a conviction for the separate crime. [L 2001, c 33, pt of §1; am L 2006, c 141, §1; am L 2012, c 192, §1; am L 2016, c 231, §42; am L 2021, c 184, §2]

§708-894 Forfeiture of property used in computer crimes. Any property used or intended for use in the commission of, attempt to commit, or conspiracy to commit an offense under this part, or which facilitated or assisted such activity, shall be forfeited subject to the requirements of chapter 712A; provided that the court shall have the discretion to require forfeiture of the property pursuant to this section if the perpetrator of the offense was a person under the age of eighteen, regardless of whether the person owned the property. [L 2001, c 33, pt of §1; am L 2021, c 184, §3]

[§708-895] Jurisdiction. For purposes of prosecution under this part, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction. [L 2001, c 33, pt of §1]

§708-895.5 Unauthorized computer access in the first degree. (1) A person commits the offense of unauthorized computer access in the first degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information, and:

(a) The offense was committed for the purpose of commercial or private financial gain;

(b) The offense was committed in furtherance of any other crime;

(c) The value of the information obtained exceeds $20,000; or

(d) The information has been determined by statute or rule of court to require protection against unauthorized disclosure.

(2) Unauthorized computer access in the first degree is a class A felony. [L 2001, c 33, pt of §1; am L 2012, c 293, §4]

§708-895.6 Unauthorized computer access in the second degree. (1) A person commits the offense of unauthorized computer access in the second degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information.

(2) Unauthorized computer access in the second degree is a class B felony. [L 2001, c 33, pt of §1; am L 2012, c 293, §5]

§708-895.7 Unauthorized computer access in the third degree. (1) A person commits the offense of unauthorized computer access in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization.

(2) Unauthorized computer access in the third degree is a class C felony. [L 2001, c 33, pt of §1; am L 2012, c 293, §6]

Federal Laws:

The Computer Fraud and Abuse Act (CFAA) is a federal law in the United States that addresses unauthorized access to computer systems. We will adhere to the provisions of the CFAA in our testing activities.

3. Authorization and Documentation:

Written authorization will be obtained from Alexander Rocco Corporation, explicitly granting permission to conduct penetration tests. The authorization document will include:

Scope of the penetration tests.

Testing parameters, including network infrastructure, systems, and applications.

Agreement on non-disclosure of sensitive information.

4. Notification to Authorities:

We will investigate whether there are any legal requirements for notifying relevant authorities before conducting penetration tests. If required, necessary notifications and permits will be obtained to ensure compliance.

5. Communication with Claudia Mae:

Maintaining transparent communication with Claudia Mae is crucial. Regular updates will be provided on the testing process, and any potential findings will be discussed with her to ensure alignment with the company's goals.

6. Non-Disclosure Agreements (NDAs):

To protect sensitive information discovered during penetration tests, a Non-Disclosure Agreement will be considered and, if deemed necessary, entered into with Alexander Rocco Corporation.

7. Understanding Network Topology:

Before initiating the tests, passive reconnaissance will be conducted to gather information about the network topology. This will involve identifying IP addresses, domain names, and other relevant network infrastructure details.

8. Documentation of Tools and Methodology:

All tools and methodologies used during the penetration tests will be documented and coordinated for approval with Claudia Mae. We will ensure the tools are legal and authorized for penetration testing.

9. Risk Assessment:

A preliminary risk assessment will be performed to identify potential vulnerabilities. The assessment will prioritize testing based on critical assets and systems.

10. Rules of Engagement:

Clear rules of engagement will be established, including:

Hours during which testing will be conducted.

Limitations to avoid any impact on business operations.

11. Contingency Planning:

A contingency plan will be developed to address any unexpected issues during the penetration tests. The plan will allow for the immediate pausing or halting of testing activities if adverse impacts are observed.