Aaron Montano

NerualEdge Innovations Risk Assessment

Introduction:

This risk assessment report was prepared by Aaron Montano on June 12, 2023 following the guidelines of the National Institute of Standards and Technology (NIST). The assessment focuses on the risks associated with a hypothetical company named NeuralEdge Innovations that develops neural link technology (brain-computer interface). NeuralEdge Innovations is a privately owned company founded in 2020 and located in Silicon Valley, California. NeuralEdge has not released any consumer products yet but has been granted permission by the FDA to conduct human trials on their current brain chip model and to collect data on the findings which will be shared with the FDA. The purpose of this assessment of NeuealEdge is to identify, categorize, and assess potential threats, vulnerabilities, and risks to the company's information systems and assets.

Scope:

The assessment covers the information systems and services provided by the NeuralEdge Innovations company. It includes an evaluation of the neural link technology, associated software, hardware, and infrastructure. The assessment aims to identify risks that could impact the confidentiality, integrity, and availability of the company's systems and assets. The assessment results will stay relevant until a significant change is made to the components of the neural link technology, the information systems implemented by NeuralEdge, or until further vulnerabilities in any of the company’s information systems are identified.

Overall Level of Risk and Findings:

Based on the assessment, the overall level of risk for the company's neural link technology is considered high. The findings indicate that several serious potential threats and vulnerabilities exist, both adversarial and non-adversarial. These risks could lead to unauthorized access, data breaches, system failures, reputational damage, and compliance issues if not adequately addressed. To identify and categorize these threats we used table E-2 and table E-3 in the NIST 800-30 document. After identifying threats, we followed the recommended steps in the NIST 800-30 document and produced tables (table 1 and 2) with our findings. These tables show the levels of risk that we assessed using qualitative measures. We chose to use qualitative measures because NeuralEdge Innovations is a hypothetical organization so we did not have any real numbers to reference. While there are numerous potential areas of risk, the level of overall risk is considered high primarily because of the devastating consequences that could come from a vulnerability in neural technology. This technology attempts to use technology to interact directly with the brain which is potentially dangerous not just in that it works with sensitive data but also to the physical health of customers. Any serious security failures of NeuralEdge innovations would lead to a significant loss in trust that could cascade into a complete business failure.

(ii) Main Body: Detailed Risk Assessment Results:

Assessment Method, Approach, Assumptions, and Constraints:

The risk assessment followed the NIST Special Publication 800-37 framework, which provides guidance for risk management. After categorizing and listing the information systems we will be evaluating, we selected 15 threats that pose a significant risk to the critical business functions related to those information systems. Lastly, we discussed some potential controls that could be used to address and mitigate the risks. Assumptions made during the assessment include considering a typical threat landscape, assuming the organization has implemented basic security controls, and that the assessment is based on current available information.

Evaluated Information Systems and Organizational Units:

The assessment covered the following organizational units and processes related to the neural link technology:

1. Neural Link Technology: The core technology that facilitates brain-computer interface communication. The company is currently testing a new brain chip that connects to an exterior LAN server.
2. Software Applications: The software used to control and interact with the neural link technology.
3. Hardware Infrastructure: The physical devices and components supporting the neural link technology.

4. Data Storage and Processing: The systems responsible for storing and processing user data collected by the neural link technology in the clinical trials.

Risk Assessment Results:
The assessment identified several risks, including both adversarial and non-adversarial threats. The risks identified are as follows:

Adversarial Threats:
1. Ransomware: Malicious software that encrypts data and demands payment for decryption.
2. Hacking: Unauthorized access to the company's systems with malicious intent.
3. Advanced Persistent Threats (APT): Targeted and sophisticated attacks aiming to gain persistent access.
4. Data Breaches: Unauthorized access to sensitive user information stored by the company.
5. Intellectual Property Theft: Theft or unauthorized disclosure of the company's proprietary technology and research.

Non-Adversarial Threats:
1. Human Errors: Mistakes made by employees that could result in system downtime or data loss.
2. Natural Disasters: Events such as earthquakes or floods that can disrupt operations and damage infrastructure.
3. Power Outages: Loss of electricity supply leading to system disruptions and potential data corruption.
4. Equipment Failures: Hardware or software failures that may cause system outages or data corruption.

5. Supply Chain Disruptions: Interruptions in the supply chain, affecting the availability of critical components.
6. Regulatory Compliance: Failure to comply with relevant laws and regulations governing the neural link technology.
7. Privacy Concerns: Unauthorized access or misuse of user data, violating privacy regulations.
8. Technology Obsolescence: Rapid technological advancements making the neural link technology outdated.
9. Financial Risks: Economic factors that could impact the company's funding or profitability.
10. Resource Depletion: Degraded processing performance due to resource depletion.

Controls:

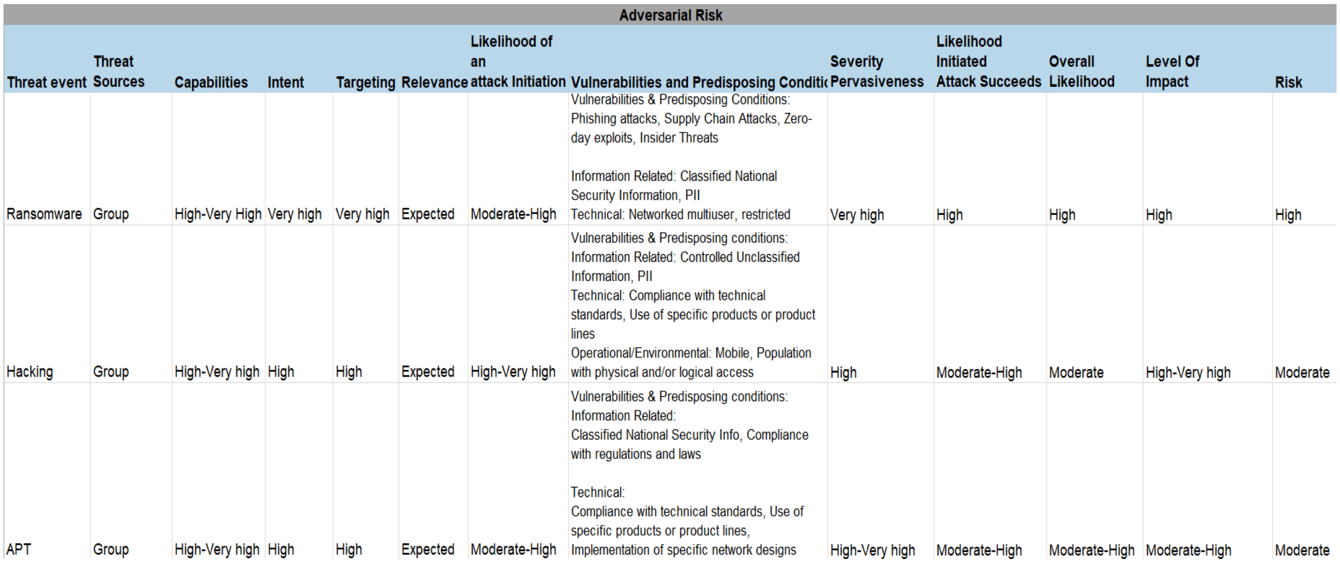
There are several options for implementing controls to lower risk in each of these 15 areas. First we will discuss the Adversarial threats listed, which have potential controls that are easier to implement. First, to address the risk of ransomware taking control of our systems, we would recommend the use of a comprehensive continuous monitoring system (CA-7) as well as a SIEM system to organize non-real-time data and potentially recognize abnormalities. Next, to control against hacking threats we would recommend the use of strict information flow enforcement (AC-4) as well as conducting penetration testing (CA-8) often. Information flow enforcement will limit where sensitive information flows in the servers and penetration testing will help clear up any avoidable security flaws. Some of the best controls we could use to mitigate the threat of Advanced Persistent Threats (APTs) are restrictions on remote access (AC-17). Even though more work is being done remotely, limiting the access of users accessing remotely and implementing specific rules for remote access will help secure our systems from advanced threats attempting to connect to and alter our systems over time. Next, to lower the risk of data breaches, we recommend NeuralEdge to implement strict access controls (AC-1) as well as a clipping level for the amount of unsuccessful login attempts (AC-7). Access controls will work well to restrict the amount of users who have access to sensitive information and lower the risk of breaches. Lastly, to minimize the risk of intellectual property theft, we recommend the use of access controls for mobile devices (AC-19) which could be used for distributing company secrets to adversaries.

One of the non-adversarial threats that poses a high risk to the organization is human error. Human errors can lead to accidental data breaches or vulnerabilities that could encourage adversarial threats to act. As mentioned previously, strict access controls will be very important in discouraging errors that could harm the company. We recommend only giving employees as much access as they need to complete their job and no more (AC-6). We also recommend intensive security training of all employees (AT-2). Some disasters are hard to predict and don't have many controls that could be implemented beforehand to discourage; these could include natural disasters, power outages, and equipment failures. For these threats, we recommend creating business continuity plans and disaster recovery plans in advance in order to enable the NeuralEdge to recover as quickly as possible and restore critical business functions following devastating events.

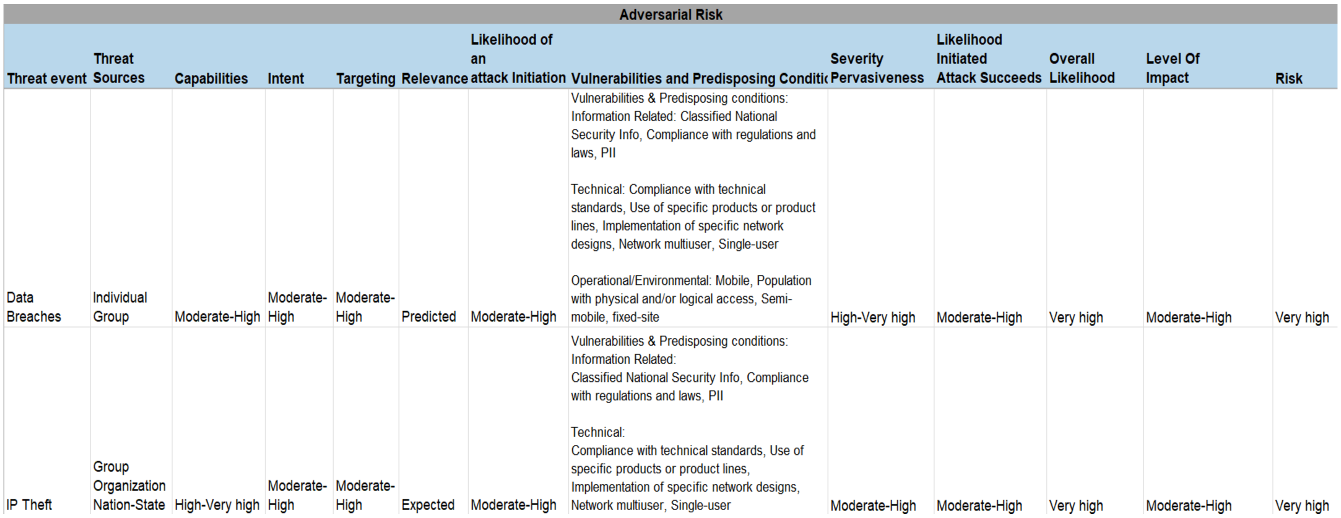
(iii) Supporting Appendices:

The following tables are included in the appendices, referencing NIST SP 800-30 document:

Table I-5 - Adversarial Risks:

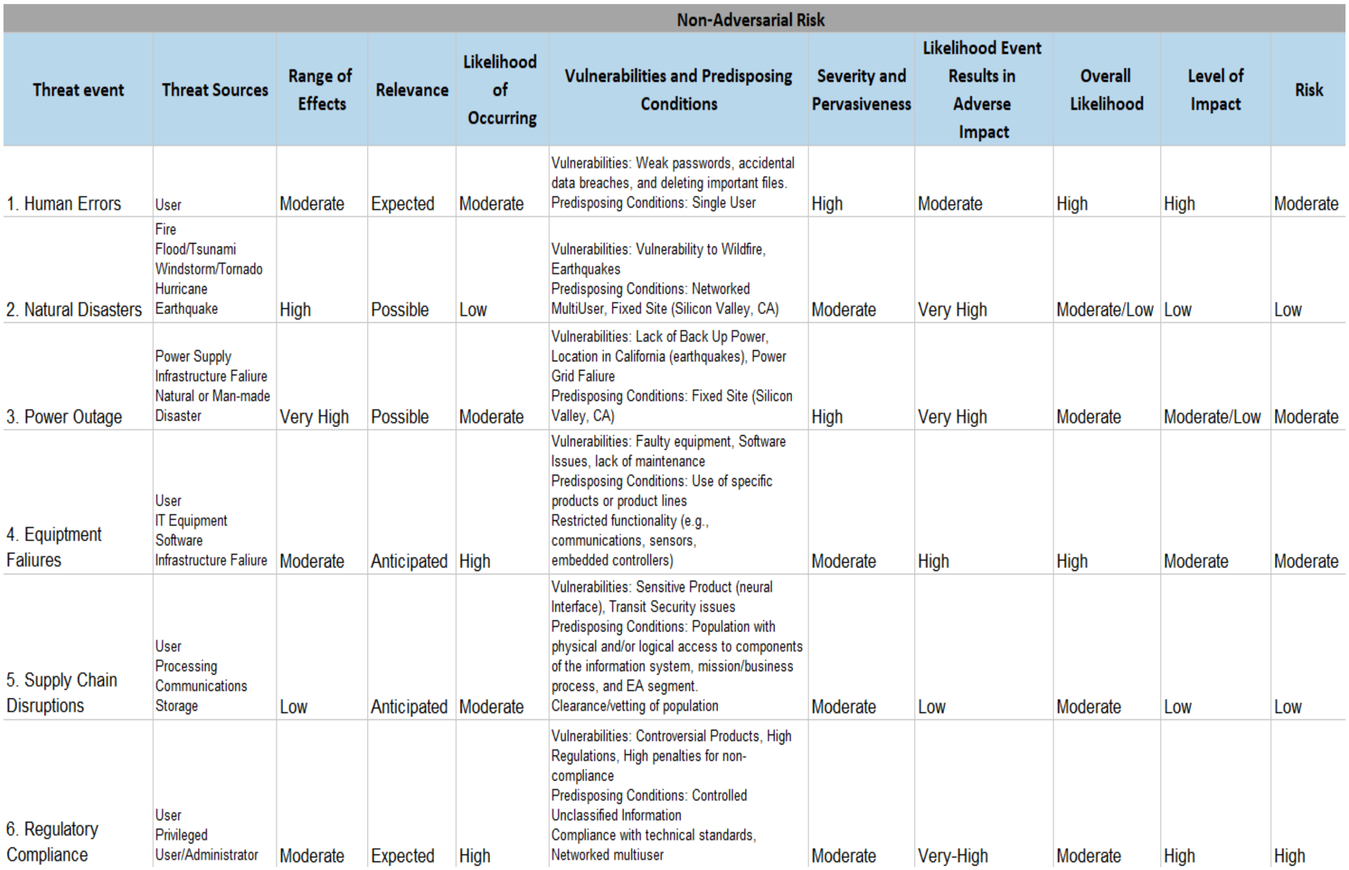


Adversarial Risk												
Threat event	**Threat Sources**	**Capabilities**	**Intent**	**Targeting**	**Relevance**	**Likelihood of an attack Initiation**	**Vulnerabilities and Predisposing Conditic**	**Severity Pervasiveness**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level Of Impact**	**Risk**
Ransomware	Group	High-Very High	Very high	Very high	Expected	Moderate-High	Vulnerabilities & Predisposing Conditions: Phishing attacks, Supply Chain Attacks, Zero-day exploits, Insider Threats Information Related: Classified National Security Information, PII Technical: Networked multiuser, restricted	Very high	High	High	High	High
Hacking	Group	High-Very high	High	High	Expected	High-Very high	Vulnerabilities & Predisposing conditions: Information Related: Controlled Unclassified Information, PII Technical: Compliance with technical standards, Use of specific products or product lines Operational/Environmental: Mobile, Population with physical and/or logical access	High	Moderate-High	Moderate	High-Very high	Moderate
APT	Group	High-Very high	High	High	Expected	Moderate-High	Vulnerabilities & Predisposing conditions: Information Related: Classified National Security Info, Compliance with regulations and laws Technical: Compliance with technical standards, Use of specific products or product lines, Implementation of specific network designs	High-Very high	Moderate-High	Moderate-High	Moderate-High	Moderate

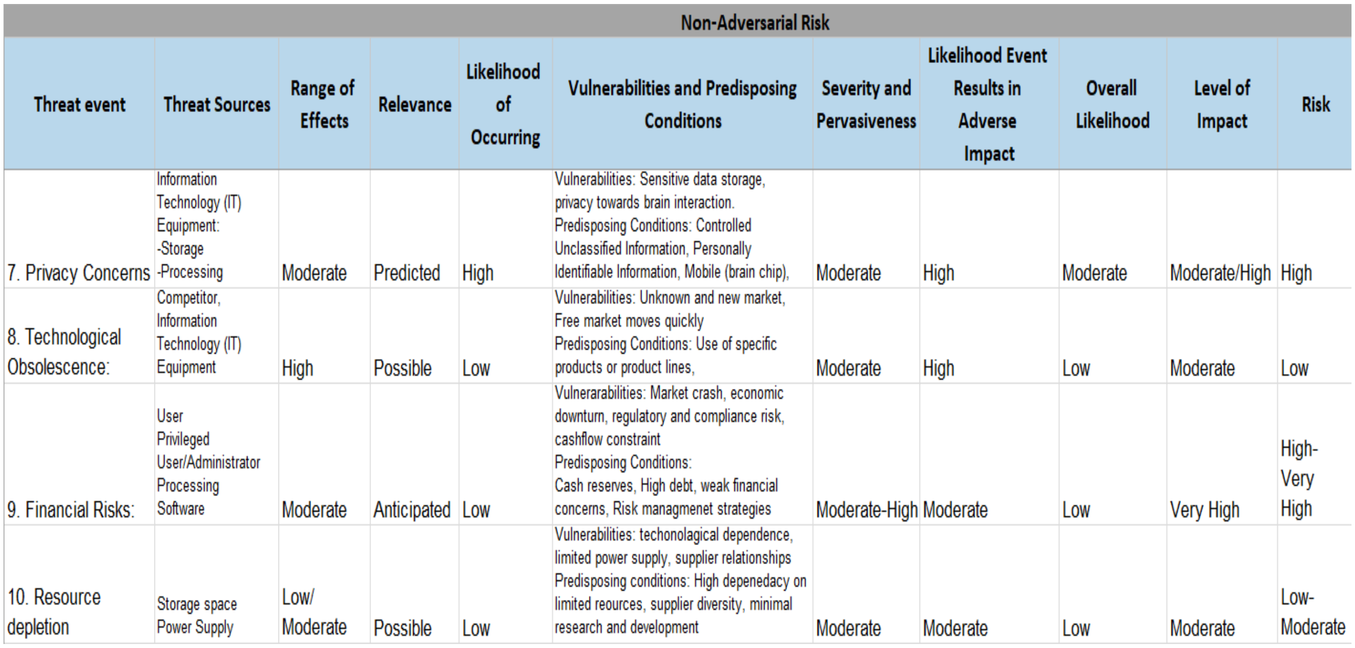


Adversarial Risk												
Threat event	Threat Sources	Capabilities	Intent	Targeting	Relevance	Likelihood of an attack Initiation	Vulnerabilities and Predisposing Conditic	Severity Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level Of Impact	Risk
Data Breaches	Individual Group	Moderate-High	Moderate-High	Moderate-High	Predicted	Moderate-High	Vulnerabilities & Predisposing conditions: Information Related: Classified National Security Info, Compliance with regulations and laws, PII Technical: Compliance with technical standards, Use of specific products or product lines, Implementation of specific network designs, Network multiuser, Single-user Operational/Environmental: Mobile, Population with physical and/or logical access, Semi-mobile, fixed-site	High-Very high	Moderate-High	Very high	Moderate-High	Very high
IP Theft	Group Organization Nation-State	High-Very high	Moderate-High	Moderate-High	Expected	Moderate-High	Vulnerabilities & Predisposing conditions: Information Related: Classified National Security Info, Compliance with regulations and laws, PII Technical: Compliance with technical standards, Use of specific products or product lines, Implementation of specific network designs, Network multiuser, Single-user	Moderate-High	Moderate-High	Very high	Moderate-High	Very high

Table I-7 - Non-Adversarial Risks:



Non-Adversarial Risk										
Threat event	Threat Sources	Range of Effects	Relevance	Likelihood of Occurring	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Event Results in Adverse Impact	Overall Likelihood	Level of Impact	Risk
1. Human Errors	User	Moderate	Expected	Moderate	Vulnerabilities: Weak passwords, accidental data breaches, and deleting important files. Predisposing Conditions: Single User	High	Moderate	High	High	Moderate
2. Natural Disasters	Fire Flood/Tsunami Windstorm/Tornado Hurricane Earthquake	High	Possible	Low	Vulnerabilities: Vulnerability to Wildfire, Earthquakes Predisposing Conditions: Networked MultiUser, Fixed Site (Silicon Valley, CA)	Moderate	Very High	Moderate/Low	Low	Low
3. Power Outage	Power Supply Infrastructure Faliure Natural or Man-made Disaster	Very High	Possible	Moderate	Vulnerabilities: Lack of Back Up Power, Location in California (earthquakes), Power Grid Faliure Predisposing Conditions: Fixed Site (Silicon Valley, CA)	High	Very High	Moderate	Moderate/Low	Moderate
4. Equipment Faliures	User IT Equipment Software Infrastructure Failure	Moderate	Anticipated	High	Vulnerabilities: Faulty equipment, Software Issues, lack of maintenance Predisposing Conditions: Use of specific products or product lines Restricted functionality (e.g., communications, sensors, embedded controllers)	Moderate	High	High	Moderate	Moderate
5. Supply Chain Disruptions	User Processing Communications Storage	Low	Anticipated	Moderate	Vulnerabilities: Sensitive Product (neural Interface), Transit Security issues Predisposing Conditions: Population with physical and/or logical access to components of the information system, mission/business process, and EA segment. Clearance/vetting of population	Moderate	Low	Moderate	Low	Low
6. Regulatory Compliance	User Privileged User/Administrator	Moderate	Expected	High	Vulnerabilities: Controversial Products, High Regulations, High penalties for non-compliance Predisposing Conditions: Controlled Unclassified Information Compliance with technical standards, Networked multiuser	Moderate	Very-High	Moderate	High	High



Non-Adversarial Risk

Threat event	Threat Sources	Range of Effects	Relevance	Likelihood of Occurring	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Event Results in Adverse Impact	Overall Likelihood	Level of Impact	Risk
7. Privacy Concerns	Information Technology (IT) Equipment: -Storage -Processing	Moderate	Predicted	High	Vulnerabilities: Sensitive data storage, privacy towards brain interaction. Predisposing Conditions: Controlled Unclassified Information, Personally Identifiable Information, Mobile (brain chip),	Moderate	High	Moderate	Moderate/High	High
8. Technological Obsolescence:	Competitor, Information Technology (IT) Equipment	High	Possible	Low	Vulnerabilities: Unknown and new market, Free market moves quickly Predisposing Conditions: Use of specific products or product lines,	Moderate	High	Low	Moderate	Low
9. Financial Risks:	User Privileged User/Administrator Processing Software	Moderate	Anticipated	Low	Vulnerarabilities: Market crash, economic downturn, regulatory and compliance risk, cashflow constraint Predisposing Conditions: Cash reserves, High debt, weak financial concerns, Risk managmenet strategies	Moderate-High	Moderate	Low	Very High	High-Very High
10. Resource depletion	Storage space Power Supply	Low/ Moderate	Possible	Low	Vulnerabilities: techonolagical dependence, limited power supply, supplier relationships Predisposing conditions: High depenedacy on limited reources, supplier diversity, minimal research and development	Moderate	Moderate	Low	Moderate	Low-Moderate