Section 4.3 Cyber Threat

Cyber Threat

As technology advances and takes a more prominent role in the public and private sectors, incidents that damage or destroy that technology become more of a threat. Cyber-attacks against infrastructure can cripple supply chains, transportation, energy production and distribution, and other technology-dependent sectors.

CHANGES SINCE 2018

+0

Declared Disasters

+5

Cyber Threat Events

COUNTIES MOST VULNERABLE

Kaua'i Honolulu Maui Hawai'i

SOCIALLY VULNERABLE POPULATION

22.3%

Of Total Population

316,257

Persons

HAZARD RANKING

Low Medium High

COMMUNITY LIFELINES

1,369

Total

CLIMATE PROJECTIONS

Climate change impacts are not known to have a direct effect on cybersecurity

Climate activists and deniers may carry out hacks to make a statement, prove a point, or benefit financially from instability

Cyber threat impacts on these physical state assets are unknown at this time.

Environmental Resources

State Buildings

Hawaiian Home Lands

Cultural Resources

Miles of State Road

CONTENTS

TABLES

FIGURES

[1] *Section Cover Photo: Stock photo*

SECTION 4. RISK ASSESSMENT

4.3 CYBER THREAT

2023 SHMP Update Changes

- The cyber threat hazard profile is new to the 2023 plan update.
- Cyber threat incidents that occurred in the State of Hawai‘i from January 1, 2018, through December 31, 2022, were researched for this 2023 SHMP Update.

4.3.1 HAZARD PROFILE

Hazard Description

A cyber-attack is an attempt to compromise system security by gaining unauthorized access to system services, resources, or information. These attacks can be carried out by individuals, organizations, or government entities by damaging or disrupting a computer or computer network or by stealing data from a computer or computer network for malicious use. Individuals or groups may use system hacking to promote their social or political ideology. Malicious software, known as ransomware, may be used to restrict access to a system or data until money is paid. Cyber-attacks can impact and/or target organizations or individuals. Tactics used in cyber-attacks are always changing and becoming more sophisticated (Hawai‘i Office of Homeland Security 2022).

A cyber incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communication systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon (The White House 2016). Such incidents (differentiated from cyber-attacks by their targeting of organizations such as critical infrastructure or governmental entities rather than individuals) can lead to numerous impacts:

- Loss or theft of computer resources
- Inappropriate access to and disclosure of personal and secure information
- Disruption of services
- Damage to networks
- High cost of remediation
- Disruption of essential operations supporting critical infrastructure
- Disruption of resources needed for emergency management

As the use of digital information expands, the state will become more vulnerable to the potential technological hazard of cyber damage. Cyber threats to critical infrastructure can be posed by anyone with the capability,

technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, state-sponsored, group-sponsored or a single rogue individual.

Location

Many systems rely on computers for day-to-day operations, including traffic signals, power plants, HVAC systems, and all the systems the State of Hawai'i depends on to operate the government. Therefore, cyber threats can occur anywhere in the state.

Previous Occurrences and Losses

Disaster and Emergency Declarations

No FEMA, USDA, or State of Hawai'i disaster declarations or proclamations related to cyber threats have been issued relevant to Hawai'i, any of its counties, or nationally. However, critical infrastructure entities, government agencies and others report persistent attempts at cyber incidents on an ongoing basis.

Event History

The State of Hawai'i, Office of Homeland Security, began receiving information regarding state-based impacts from cyber incidents in 2021. As not all cyber incidents have mandated reporting requirements, this timing and the reporting received should not be taken as anything more than a snapshot of potential cyber incident activity. Additionally, impacts reported include those resulting from broader-based incidents that impacted entities across the globe. Finally, the timing of such incidents is fluid as threat actors may infiltrate impacted systems long before the entity becomes aware and, indeed, may remain within affected systems even after the entity believes they have remediated the incident. Incidents tabled below are indicative of type, but not of numbers of reports or impacted entities. Table 4.3-1 summarizes significant incidents in the state since 2018.

Table 4.3-1. Cyber Incidents from 2018 to 2022

Date of Incident	Event Type	Counties Affected	Impacts
2021	Vulnerability Exploitation	Honolulu	IT disruption, resource diversion (to mediation), reputational
2021	Ransomware	Honolulu	IT disruption, resource diversion (to mediation), reputational
2022	Vulnerability Exploitation	Maui	IT disruption, resource diversion (to mediation), reputational
2022	Targeted Phishing	Honolulu	None reported
2022	Denial of Service	Honolulu	Outward-facing website availability.

Source: Hawai'i Office of Homeland Security

Probability of Future Hazard Events

Overall Probability

There are over 2,200 cyber-attacks every day in the United States, which breaks down to nearly 1 cyber-attack every 39 seconds (Security Magazine 2023). Globally, 65 percent of board members felt that their organization was at risk of a cyber-attack (CPO Magazine 2022). A new organization is hit by ransomware every 14 seconds (Cloudwards 2022). There has been an 87 percent increase in malware infections over the last 10 years (Vuleta

2022). Aside from what has become mantra for cybersecurity practitioners (it's not a matter of if, but when), the probability of cyber incidents is only truly discernable at this point in time at the entity level, such as a singular business or organization. While it is the ambition of the state to have that depth of understanding with regards to its ciritcal infrastructure sectors and functions, it does not have that presently.

Climate Change Impacts

Climate change impacts are not known to have a direct effect on cybersecurity. However, climate change may impact the frequency or severity of cyber-attacks as valuable resources become scarcer. The increased use of computing resources due to a surge in remote work and supercomputing also contributes to climate change. People who no longer trust financial institutions due to prominent hacks and leaks are shopping and trading online or putting their money in cryptocurrencies. (Brode 2022).

An indirect impact of climate change on cyber threats could be politically based. Eco-terrorist hackers might target companies or agencies with whose policies or practices they do not agree.

Climate change impacts are not projected to change the location, intensity, frequency, or duration of cyber threats.

EXTENT

Cyber threats can vary in their severity based on the systems affected by an attack, the warning time, and the ability to preempt an attack (Cybersecurity & Infrastructure Security Agency n.d.). In 2016, the White House released a schema describing the extent of cybersecurity threats. The schema defines six levels of cyber incidents (Level 0–Level 5) as shown in Figure 4.3-1. Each level describes the incident's potential to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. An incident that ranks at a Level 3 or above is considered "significant" (The White House 2016).

Costs associated with cyber attacks have varied widely across industries and year over year. Healthcare data breach costs increased from an average of $7.13 million in 2020 to $9.23 million in 2021, a 29.5 percent increase. Costs in the energy sector decreased from $6.39 million in 2020 to $4.65 million in 2021. Costs surged in the public sector, which saw a 78.7 percent increase in cost, from $1.08 million to $1.93 million (IBM Security 2021).

The severity and timing of cyber threats are impossible to predict. There may be no warning. Some cyber incidents take weeks, months or even years to be discovered and identified (FEMA 2021).

4.3.2 VULNERABILITY ASSESSMENT

Overall, it is difficult to quantify potential losses due to cyber threat incidents because of the many variables that must be considered, including but not limited to the target of the threat and the time it takes to secure or restore information systems. Potential impacts may be local, regional, or statewide, national, or international depending on the magnitude of the event and level of service disruptions. A qualitative assessment is discussed below.

Figure 4.3-1. Cybersecurity Threat Levels

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Assessment of State Vulnerability and Potential Losses

This section discusses statewide vulnerability of exposed state assets (state buildings and roads) and critical facilities to cyber threats.

State Assets

All state-owned and leased facilities are vulnerable to cyber threats. While the physical structures of the buildings are typically not at risk, information systems and data storage within those buildings are vulnerable, as are the business and/or operation functions that they support. State computer networks may contain sensitive information and data, making them targets for cyber-attacks. Many assets are also essential to daily operations with computer networks to monitor and control functions throughout the state. A large-scale cyber incident could lead to significant economic losses to impacted state departments and agencies, businesses, and other dependent or interdependent industries.

Community Lifelines and Critical Facilities

All community lifelines and critical facilities across all critical infrastructure sectors are vulnerable to cyber threats. Interruption of services may impact facilities that need to be in operation in response to a cyber threat.

Assessment of Local Vulnerability and Potential Losses

This section provides a summary of vulnerability and potential losses to socially vulnerable and total populations, general building stock, and environmental resources and cultural assets. Each county's vulnerability and potential loss will vary greatly depending the target and the time it takes to secure or restore information systems. The local HMPs were reviewed, and their discussions of cyber threats are summarized below:

- Kaua'i County—The 2021 County of Kaua'i Multi-Hazard Mitigation and Resilience Plan does not discuss cyber threats in the risk assessment, but it includes one mitigation action to enhance cyber security measures across government agencies.
- City and County of Honolulu—The 2020 Multi-Hazard Pre-Disaster Mitigation Plan for the City and County of Honolulu does not address cyber threats.
- Maui County—The 2020 County of Maui Hazard Mitigation Plan Update does not address cyber threats.
- Hawai'i County—The 2020 County of Hawai'i Multi-Hazard Mitigation Plan provides a brief qualitative discussion of both cyber-attacks and cyberterrorism.

Socially Vulnerable and Total Populations

Because the majority of the population of the State of Hawai'i is considered to be exposed and vulnerable to cyber threats, the exposed population in socially vulnerable communities is equal to the statewide population. While socially vulnerable communities may not have access to devices that provide access to cyber threats (though unlikely given the ubiquitous nature of cellphones today), these communities likely rely heavily on agencies and programs that do, which could worsen the impacts of cyber events on these communities.

Cyber-attacks affect organizations and individuals alike. Exposure of personal information can result in individuals facing economic hardship from fraud, putting people at risk of poverty. For those already experiencing impoverishment, a cyber threat can compound the situation. Smaller businesses may face greater proportional impacts from cyber-attacks, as they have fewer resources to develop suitable cybersecurity protocolsto prevent cyber incidents and have fewer resources to recover from a loss of functionality. The vulnerable populations most susceptible to cyber threats are adults over 75 (Gaskell 2021).

General Building Stock

The general building stock is not at risk from cyber threats, but the information systems and data storage within those buildings are vulnerable, as are the business and/or operation functions that they support.

Environmental Resources

A cyber threat does not have direct impacts to environmental resources; however, secondary impacts to the environment can occur. If a water or wastewater treatment facility is targeted and operations are interrupted, outflows may result which could pollute land and water environments, or negatively impact the populations that rely on them.

Cultural Assets

Meticulous records and digital files can be swept away, impossible to recover or replace. Within the Comprehensive Cultural Property Risk Analysis Model (CPRAM), cyber-attacks have been identified as a root cause of a dissociation risk to collections, specifically the loss of database collection information.

Future Changes that May Impact State Vulnerability

Understanding future changes that impact vulnerability in the state can assist in planning for future development and ensuring that appropriate mitigation, planning, and preparedness measures are in place. The State of Hawai'i considered the following factors to examine potential conditions that may affect hazard vulnerability:

- Potential or projected development or business growth
- Projected changes in population
- Other identified conditions as relevant and appropriate

An estimated 2,883 square miles of buildable land is available for development statewide. Because the entire state is vulnerable to cyber threats, any type of development of any of this land will be susceptible to damage and impacts from this hazard. Likewise, any growth of businesses, particularly those providing critical functions, like data centers or data service providers, expands the environment of potential cyber-attack targets.