5.4.2 Cyber Security

This section provides a profile and vulnerability assessment of the cyber security hazard.

Profile

This section presents the cyber security description, extent, location, previous occurrences and losses, and probability of future occurrences.

Description

A cyber incident involves either the theft or modification of information on government agency computer systems, or a system compromise with the potential to disrupt essential services. A system compromise can impact one or more government agencies, a private utility, or specific Critical Infrastructure/Key Resources (CIKR) such as the power grid, public transportation systems, and wireless networks (NYC Emergency Management 2019).

Cyber-attacks differ by motive, attack type and vector, and perpetrator profile. Motives for cyber-attacks can vary, ranging from the pursuit of financial gain to political or social aims. Cyber threats are difficult to identify and comprehend. Types of threats include viruses erasing entire systems, intruders breaking into systems and altering files, intruders using someone's personal computer to attack others, or intruders stealing confidential information. The spectrum of cyber risks is limitless, with threats having a wide-range of effects on the individual, community, organizational, and national threat (NYC Emergency Management 2019). These risks include:

- Organized cybercrime, state-sponsored hackers, and cyber espionage can pose national security risks to the U.S.
- Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.
- Vulnerability to data breach and loss increases if an organization's network is compromised. Information about a company, its employees, and its customers can be at risk.
- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the internet are vulnerable to intrusion. Personal information may be at risk without proper security (NYC Emergency Management 2019).

Cyber terrorism is the use of existing computers and information, particularly over the Internet, to cause physical or financial harm or a severe disruption of infrastructure service. Transportation, public safety, and utility services are all critical, and are highly dependent on information technology. The motive behind such disruptions can be driven by religious, political, or other objectives. Three kinds of attacks that can be conducted on computers include attacks of physical means, electronic means, and attacks using malicious code (Waldron 2011). Specifically, these types of include:

- Directing conventional kinetic weapons against computer equipment, a computer facility, or transmission lines to create a physical attack that disrupts the reliability of equipment.
- The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse (EMP), can be used to create an electronic attack (EA) directed against computer equipment or data transmissions. By overheating circuitry or jamming communications, an EA disrupts the reliability of equipment and the integrity of data.

- Malicious code can be used to create a cyber-attack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyber-attack can disrupt the reliability of equipment, the integrity of data, and the confidentiality of communications (Wilson and Clay 2007).

Cyber terrorists typically have two broad motivations to carry out an attack. These motivations include:

- Effects-based: Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism.
- Intent-based: Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage (Rollins and Clay 2007).

Table 5.4.2-1. Perpetrator Categories for Cyber-attacks

Category	Category Description	Description of Attack
External	Outside the victim organization	Attacks—which can be perpetrated by subgroups including organized crime, nation-state or state-affiliated entities, unaffiliated individuals, activists, former employees, acquaintances, competitors, or customers—can take any number of forms.
Internal	Inside the victim organization	These attacks have usually been malicious, for the purposes of financial gain, though some were the result of breaches due to careless or accidental data exposure. Internal actor subgroups include system admin, end-user, doctor or nurse, developer, manager, executive, cashier, finance, and human resources.
Partner	Third party sharing a business relationship with the victim	The least common of the three perpetrator categories and often unintentional. Example: a courier losing a device containing sensitive data

Source: Verizon Wireless DBIR 2018

In terms of specific attacks on computers, cyber terrorists have the ability to attack several types of computer systems in a variety of ways. The systems are summarized in Table 5.4.2-2.

Table 5.4.2-2. Computer Systems that can be Attacked

Computer System	Description
All system and network devices BIND weaknesses	The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of Domain Name Service (DNS) by which systems on the Internet are located by name, without having to know specific Internet protocol (IP) addresses. In a typical example of a BIND attack, intruders erase system logs and install tools to gain administrative access. They then compile and install Internet Relay Chat (IRC) utilities and network scanning tools, which are used to scan more than a dozen class-B networks in search of additional systems running vulnerable versions of BIND. In a matter of minutes, they can use the compromised system to attack hundreds of remote systems.
Vulnerable Common Gateway Interface (CGI) programs and application extensions (such as ColdFusion) installed on Web servers (multiple UNIX and Linux systems)	Most Web servers support CGI for data collection and verification. Intruders are known to have exploited vulnerable CGI programs to vandalize Web pages and steal credit cards.
RPC weaknesses (all Web servers)	Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely used to access network services such as shared files in the Network File System (NFS). There is compelling evidence that the vast majority of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had RPC vulnerabilities. In 1998, the broadly successful attack on U.S. military systems during the Solar Sunrise

Computer System	Description
	incident also exploited an RPC flaw found on hundreds of Department of Defense systems.
RDS security hole in Microsoft IIS (multiple UNIX and Linux systems)	Programming flaws in Microsoft's Internet Information Server (IIS) used to host websites deployed on Microsoft Windows NT and Windows 2000 are employed by malicious users to run remote commands with administrator privileges. Experts who developed the "Top Ten" list of the most exploited internet security flaws believe that exploits of other IIS flaws, such as .HTR files, are at least as common as exploits of Remote Desktop Services (RDS).
Sadmind (Solaris machines only)	Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access to hostile parties.
User IDs, especially root/administrator with no or weak passwords (UNIX, Windows, and Macintosh systems)	Some systems come with "demo" or "guest" accounts with no passwords or with widely- known default passwords. Service workers often leave maintenance accounts with no passwords, while some database management systems install administration accounts with default passwords. In addition, busy system administrators often select system passwords that are easily guessable ("love," "money," "wizard" are common) or use a blank password. Many attackers try default passwords and then try to guess passwords before resorting to more sophisticated methods.
IMAP and POP buffer overflow vulnerabilities or incorrect configuration (all systems)	Internet message access protocol (IMAP) and Post Office Protocol (POP) are popular remote access mail protocols, allowing users to access their e-mail accounts. The "open access" nature of these services makes them especially vulnerable to exploitation because openings are frequently left in firewalls to allow for external e-mail access. Attackers who exploit flaws in IMAP or POP often gain instant root-level control.
Default SNMP community strings set to "public" and "private" (multiple UNIX and Linux systems)	The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices, ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption creates one level of security vulnerability, but the default community string used by the vast majority of SNMP devices is "public," with a few clever network equipment vendors changing the string to "private," which presents a greater security risk. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely.

Source: NJOEM 2019

In addition to the motivations for cyber terrorism and the vulnerable systems, cyber-attacks can be further divided by the complexity of the attack. The categories of attacks include:

- Simple-Unstructured: Simple-unstructured attacks are the most common. These are amateurish attacks with relatively minimal consequences.
- Advanced-Structured: Advanced-structured attacks are more sophisticated and consequential and have a greater emphasis on targeting victims prior to an attack, resulting in a more debilitating effect.
- Complex-Coordinated: Complex-coordinated attacks are the most advanced and most troublesome type of attack where success could mean a network shutdown.

Because virtually all critical systems are reliant upon computer systems, the secondary hazards that could result from a cyber terrorism attack could be devastating. For example, many of New York's roadway systems rely on sophisticated traffic control systems that prevent gridlock and accidents daily. Without these systems, the risk of not only auto accidents increases but also hazardous materials in-transit incidents. Additionally, a cyber-attack on a nuclear power plant could have devastating consequences should the plant suffer an intentional catastrophic failure. A cyber-attack could also completely incapacitate the communications infrastructure not only in New York but across the United States, leading to disturbing secondary consequences and hazards. Public Safety Answering Points could be targeted by cyber-attacks, and if affected, there could be significant impacts to public safety response and dispatching of emergency services.

Because the power grid is also largely controlled by computer systems, a widespread power outage is also a possibility. A failure of the power grid would impact individuals reliant on power such as those with medical needs. The number of critical systems reliant on computer systems are numerous, thus disruption of one or more of the systems would cause severe secondary-cascading hazards. Secondary impacts could also affect private structures and systems within them: HVAC systems, life support systems, and security systems. Power outage caused from cyber-attacks can also affect individuals who are dependent on medical equipment.

Since cyber security is a fairly new concept, there are limited regulations in place. The United States Department of Homeland Security (DHS) recognizes the threat of a potential cyber-attack and has established the Cyber & Infrastructure (CISA) Division to address cyber related threats. CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations (US Department of Homeland Security N.D.).

In 2019, Suffolk County undertook a Cybersecurity Project to determine any existing vulnerabilities to cyber-attacks, as well as what recommendations should be implemented to protect its physical and digital infrastructure. As a result of this effort, additional trainings and tabletop exercises have taken place.

Extent

The magnitude of extent of an incident will vary greatly based on the extent and duration of the impact. Additionally, the extent will vary based upon which specific system is affected by an attack, the warning time, and ability to preempt an attack.

A cyber-attack can affect a variety of sectors with potentially severe consequences. The following areas may be affected by an attack:

- Android: Malicious software designed to exploit the Android operating systems (OS) running on smartphones, tablets, and other devices. Some variants of Android malware have the capability of disabling the device, allowing a malicious actor to remotely control the device, track the user's activity, lock the device, or encrypt or steal personal information transmitted from or stored on the device. As users are increasingly turning to mobile devices for both business and personal use, cyber threat actors are devoting their efforts to developing malware designed to compromise the device software.
- Botnets: A group of internet-connected computers and devices that have been infected by malware that allows a malicious actor to control them remotely. The malicious actor then uses the botnet for nefarious purposes such as sending spam email, stealing data, spreading additional malware infections to other devices, generating illicit advertising revenue through click-fraud, mining cryptocurrencies, or conducting distributed denial-of-service (DDoS) attacks. In the cases where botnets are used to conduct DDoS attacks, these infected devices are used to generate an excessive amount of network traffic designed to overwhelm a website, server, or online service to the point that legitimate users cannot access it.
- Exploit Kits: Toolkits that automate the exploitation of vulnerabilities in popular software applications to maximize successful infections and serve as a platform to deliver malicious payloads such as Trojans, spyware, ransomware, and other malicious software. Most users will encounter EKs from visiting seemingly legitimate, high-traffic websites that either contain links to EKs embedded within malicious advertising (malvertising) or have malicious code hidden directly within the website itself. Malicious URLs linking to EKs are commonly distributed through spam email and spear-phishing campaigns.
- ICS: A collective term for several types of control systems and other equipment used to operate and/or automate industrial processes and includes supervisory control and data acquisition (SCADA) systems – often incorrectly used interchangeably with ICS – and distributed control systems (DCS).

- IOS: Malicious software designed to exploit Apple's iOS operating system running on smartphones, tablets, and other devices. Some variants of iOS malware have the capability of disabling the device, allowing a malicious actor to remotely control the device, track the user's activity, lock the device, or encrypt or steal personal information transmitted from or stored on the device. As users are increasingly turning to mobile devices for both business and personal use, cyber threat actors are increasingly devoting their efforts to developing malware designed to compromise mobile devices, including operating systems, like iOS, and applications, like those available in the App Store. Android devices have historically seen more malware threats than iOS largely due to the open-source operating system; however, malware specifically targeting iOS has increased in the last two years.
- MACOS: Though the majority of known malware targeting operating systems are made to exploit Microsoft Windows, devices running macOS are vulnerable as well. Furthermore, as macOS has become increasingly popular, more malware has been created to target macOS. More macOS malware was discovered in the second quarter of 2017 than in all of 2016.
- Point of Sale (PoS): Malicious software designed to steal credit and debit card data from payment processing systems, known as point-of-sale (PoS) terminals.
- Ransomware: Malicious software (malware) that attempts to extort money from victims by restricting access to a computer system or files. The most prevalent form of this profit-motivated malware is crypto-ransomware, which encrypts files into encoded messages that can only be decrypted (decoded) with a key held by the malicious actor.
- Trojans: A type of malware that, unlike viruses and worms, does not self-replicate. Named after the mythological wooden horse used to sneak Greek warriors through the gates of Troy, trojans are often disguised as legitimate software to avoid detection or trick users into installing the trojan onto their system. Users can be exposed to trojans through numerous vectors, such as clicking on links or opening attachments in phishing emails, other forms of social engineering, malicious advertising (malvertisting), or by visiting compromised websites, known as drive-by downloads. Once a trojan executes, it often downloads other malware onto the system or provides an attacker with a backdoor to gain access and conduct further malicious activity, such as stealing, deleting, or modifying data (NJCCIC 2019).

The extent, nature, and timing of cyber incidents are impossible to predict. There may or may not be any warning. Some cyber incidents take a long time (weeks, months or even years) to be discovered and identified (FEMA 2019). The magnitude of severity of an incident will vary greatly based on the extent and duration of the impact. The extent will also vary based upon which specific system is affected by an attack, the warning time, and the ability to preempt an attack.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) created the Cyber Alert Level Indicator. It shows the current level of malicious cyber activity and reflects the potential for, or actual damage. There are five cyber alert levels: low, guarded, elevated, high, and severe. Each level is indicated by a color. The following is additional information regarding these levels:

- **Low** – Indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.

- **Guarded** – Indicates a general risk of increased hacking, virus, or other malicious activity. The potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.

- **Elevated** – Indicates a significant risk due to increased hacking, virus, or other malicious activity which compromises systems or diminishes service. At this level, there is known vulnerabilities that are being

exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.

- **High** - Indicates a high risk of increased hacking, virus or other malicious cyber activity which targets or compromises core infrastructure, causes multiple service outages, multiple system compromises or compromises critical infrastructure. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.

- **Severe** - Indicates a severe risk of hacking, virus or other malicious activity resulting in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or widespread level of damage or disruption of Critical Infrastructure Assets.

The United States Federal Cybersecurity Centers, in coordination with departments and agencies with a cybersecurity or cyber operations mission, adopted a common schema for describing the severity of cyber incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework for evaluating and assessing cyber incidents to ensure that all departments and agencies have a common view of the:

- The severity of a given incident;
- The urgency required for responding to a given incident;
- The seniority level necessary for coordinating response efforts; and
- The level of investment required of response efforts (United States Federal Cybersecurity Centers, N.D.).

The table below depicts several key elements of the schema.

Table 5.4.2-3. Cyber Incident Severity Schema

	General Definition	Observed Actions	Intended Consequence[1]
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.	Effect	Cause physical consequence
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.		Damage computer and networking hardware
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.	Presence	Corrupt or destroy data
			Deny availability to a key system or service
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement	Steal sensitive information
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.		Commit a financial crime
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.	Preparation	Nuisance DoS or defacement

Source: United States Federal Cybersecurity Centers N.D.

Location

Cyber threats to critical infrastructures 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 or a single rogue element. Terrorists, insiders, disgruntled employees, and hackers are included in this profile. The fact that most of the nation's vital services are delivered by private companies creates a significant challenge in assigning the responsibility for protecting our critical infrastructures from cyber-attacks. Across New York, countless systems rely on computers for day-to-day operations including but not limited to traffic signals, power plants, HVAC systems, as well as systems responsible for ensuing New York's State government can operate.

Across the United States, various industries have been impacted by cyber incidents and breaches. The table below shows the volume of cyber incidents and breaches affecting victim industries across the United States

Table 5.4.2-4. Security Incidents and Breaches by Victim Industry and Organization Size in 2017

	Incidents				Breaches			
	Large	Small	Unknown	Total	Large	Small	Unknown	Total
Accommodation (72)	40	296	32	368	31	292	15	338
Administrative (56)	7	15	11	33	5	12	1	18
Agriculture (11)	1	0	4	5	0	0	0	0
Construction (23)	2	11	10	23	0	5	5	10
Education (61)	42	26	224	292	30	15	56	101
Entertainment (71)	6	19	7,163	7,188	5	17	11	33
Financial (52)	74	74	450	598	39	52	55	146
Healthcare (62)	165	152	433	750	99	112	325	536
Information (51)	54	76	910	1,040	29	50	30	109
Management (55)	1	0	1	2	0	0	0	0
Manufacturing (31-33)	375	21	140	536	28	15	28	71
Mining (21)	3	3	20	26	3	3	0	6
Other Services (81)	5	11	46	62	2	7	26	35
Professional (54)	158	59	323	540	24	39	69	132
Public (92)	22,429	51	308	22,788	111	31	162	304
Real Estate (53)	2	5	24	31	2	4	14	20
Retail (44-45)	56	111	150	317	38	86	45	169
Trade (42)	13	5	13	31	6	4	2	12
Transportation (48-49)	15	9	35	59	7	6	5	18
Utilities (22)	14	8	24	46	4	3	11	18
Unknown	1,043	9	17,521	18,573	82	3	55	140
Total	**24,505**	**961**	**27,842**	**53,308**	**545**	**746**	**915**	**2,216**

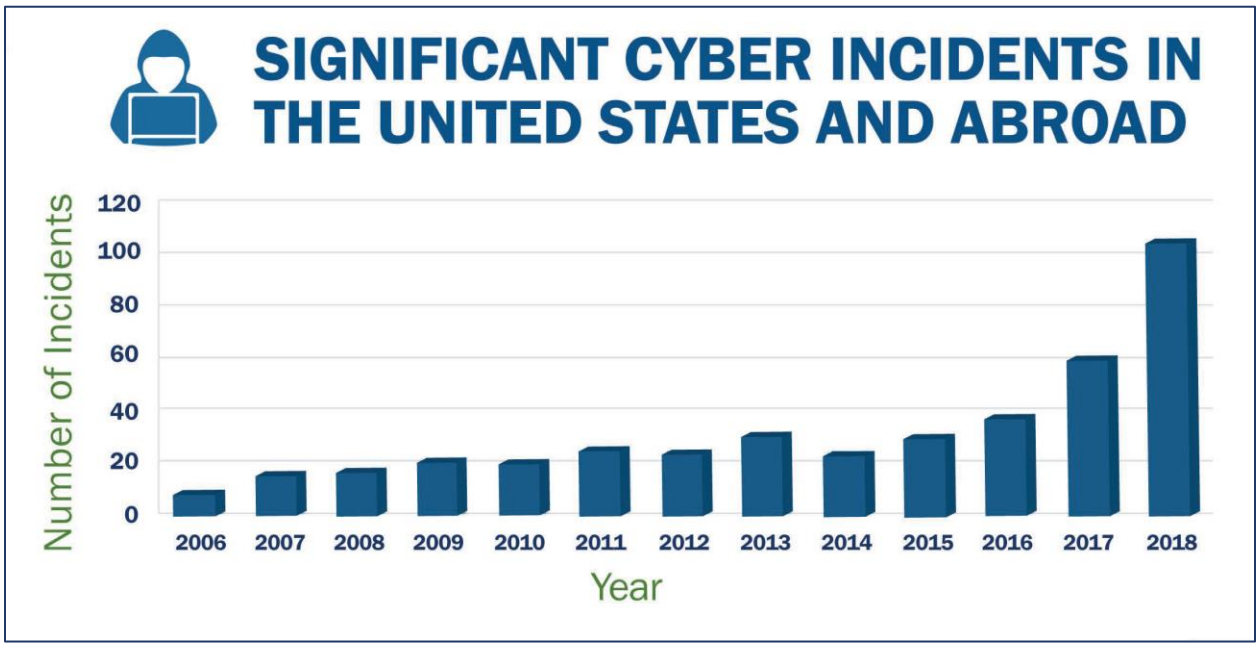
Source: Verizon Wireless DBIR 2018

Previous Occurrences and Losses

While no major direct cyber-attacks have affected Suffolk County, as mentioned, cyber terrorism is an emerging hazard that can impact the State's computer infrastructure and the systems and services that are provided to the public. Across the United States and globally, concerns over cyber terrorism are growing (U.S. Department of Homeland Security 2019). Many smaller-scale attacks have occurred.

There have been no FEMA disaster declarations related to a cyber-attack to date. According to the U.S. Department of Homeland Security, significant cyber incidents have risen steadily in the last 5 years in the United States and abroad.

Figure 5.4.2-1. Significant Cyber Incidents in the United States and Abroad



Source: U.S. Department of Homelands Security 2019

Probability of Future Occurrences

The Department of Homeland Security has noted that cyber incidents are on the rise globally (U.S. Department of Homeland Security 2019). The level of success of an attack and the subsequent damage it can create will vary greatly. With the growing popularity and use of computers, there has been a significant increase in investigations where computers are being utilized for the commission of fraud and identify theft. The probability of a cyber-attack that will affect Suffolk County is difficult to calculate; however, it is estimated that Suffolk County will continue to experience direct and indirect impacts of cyber-attacks.

In Section 5.3, the identified hazards of concern for Suffolk County were ranked. The probability of occurrence, or likelihood of the event, is one parameter used for hazard rankings. Based on historical records and input from the Planning Committee, the probability of occurrence for cyber-attacks in the County is considered 'frequent'.

Climate Change Impacts

Because cyber-attacks are human-caused, there are no climate change impacts associated with this hazard.

Vulnerability Assessment

To understand risk, a community must evaluate what assets are exposed and vulnerable to the identified hazard. The following discusses Suffolk County's vulnerability, in a qualitative nature, to the cyber security hazard. Table 5.4.2-5 summarizes potential impacts on population, facilities, economy and the environment.

Table 5.4.2-5. Cyber Attack Impact Summary

Consideration	Description
General Public	No direct loss of life is expected from an attack. Indirect injuries or deaths may result from secondary effects to critical life-sustaining resources such as energy and water.
Response Personnel	No direct affects to the health and safety of response personnel are expected; however, critical response systems may be affected.
Property, Facilities and Infrastructure	Effects can range from annoyance to complete shutdown of critical infrastructures caused by infiltration of supervisory control and data acquisition (SCADA) systems. Secondary effects could disturb public welfare and property by denying services or providing false readings.
Economic	Because of the heavy reliance on the electronic transfer of economic and commercial information, the economy could be affected by communication difficulties.
Environment	Generally, cyber terrorism has no direct effect on the environment; however, the environment may be affected should a release of a hazardous material occur because of critical infrastructure failure.
Continuity of Operations	Severe effects to continuity of operations could result if a cyber-attack reached critical operational systems or systems that were needed to carry out the operation.
Reputation of the Entity	If exposed vulnerabilities were known and not reduced or eliminated before the attack, the entity would suffer major damage to their reputation for not taking action before the incident.
Delivery of Services	Cyber-attacks may affect delivery of services if the system was infiltrated and directed to malfunction by self-destructing or overloading.
Regulatory and Contractual Operations	Cyber-attacks would have no significant effect on regulatory or contractual obligations, other than the possible elimination of electronic records, which would affect both.

Source: NJOEM 2019

Impact on Life, Health and Safety

Although there is no direct loss of life expected from a cyber-attack, all residents in Suffolk County are exposed to this hazard. Commonly stolen personal information includes name, social security number, and drivers' license information. Because it is difficult to predict the particular target of cyber terrorism, assessing vulnerability to the hazard is also difficult. Generally, all populations who directly use a computer or those receiving services from automated systems are vulnerable to cyber terrorism. Although all individuals in Suffolk County are vulnerable to an attack, certain types of attacks would impact specific segments of the population.

If the cyber-attack targeted the State's power or utility grid, vulnerable populations could be most impacted. For example, individuals with medical needs are vulnerable because many of the life-saving systems they rely on require power. Also, if an attack occurred during months of extreme hot or cold weather, the County's elderly population (those 65 years of age and older; i.e., 239,285 total persons in the County) would be vulnerable to the effects of the lack of climate control. These individuals would require shelter or admission to a hospital. Other populations vulnerable to the secondary effects of cyber terrorism are young children.

Furthermore, households located near vulnerable facilities could experience greater impacts of a cyber-attack. If a cyber-attack targeted a facility storing or manufacturing hazardous materials, individuals living adjacent to these facilities would be vulnerable to the secondary effects, should the attack successfully cause a critical failure at that facility. Individuals living within 10 miles of a nuclear power plant would be vulnerable should an attack occur at that caused a failure at a facility.

Impact on General Building Stock

There are 533,279 buildings in Suffolk County at risk of experiencing impacts from a cyber-attack. A cyber-attack can impact buildings ranging from annoyance to complete shutdown caused by infiltration of supervisory

control and data acquisition (SCADA) systems. Secondary effects could disturb public welfare and property by denying services or providing false readings (NJOEM 2019). If services are disrupted by attacks, cyber incidents can cause damage to physical assets. Should a cyber attack target fire suppression systems, these structures are likely to be at higher risk for structural fire. In many cases, attacks on these systems are initially undetectable, and it may be some time before it is known that system impairment or failure is the result of a cyber-event (NYC Emergency Management 2019).

Impact on Critical Facilities

Critical facilities and lifelines are vulnerable to cyber-attacks based on the significance of the facilities, and the potential to interrupt critical systems in the County. As previously mentioned, many critical facilities are reliant upon computer networks to monitor and control critical functions. This can include utilities, public safety facilities, medical facilities, or government buildings. A cyber-attack could result in catastrophic failure of one of these facilities. The power grid is reliant upon computer systems to distribute power to the State. An attack could disrupt power to millions of New York residents. This is just one example of how critical facilities are vulnerable to cyber-attacks. Given the importance of critical facilities to daily living activities, critical facilities are highly vulnerable to cyber-attacks.

Impact on the Economy

Cyber-attacks can have a damaging effect on public trust in systems that are traditionally considered stable and secure. Cyber-attacks can also have extensive economic impacts. Companies and government services can lose large sums of unrecoverable revenue from site down-time and possible compromise of sensitive confidential data. Further, the cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. Cybercrimes can cause damage to a company's brand and reputation, consumer losses from fraud, the opportunity costs of service disruption and "cleaning up" after cyber incidents, and the cost of increased spending on cybersecurity (McAfee 2013).

Given the proliferation of electronic commerce and the reliance on electronics, virtually all elements of New York's economy are vulnerable to cyber-attacks. The secondary impacts of a significant attack would be devastating to the economy. For example, an attack that caused the loss of power to hundreds of thousands of businesses during peak holiday shopping months could potentially cost the State millions of dollars in tax revenue if these businesses were closed. Additionally, a disruption in New York's manufacturing, agricultural, or tourism sectors would have devastating impacts on the economy. While it is difficult to quantitatively measure the economic impact of a cyber terrorism attack, it is safe to say that the impact would be great, thus the economy is vulnerable to cyber terrorism attacks.

According to FEMA, cyber-attack victims in the United States lost a collective $1.33 billion to cyber actors in 2016 (FEMA 2019). However, this estimate could be understated. In the United States, the costs of cyber terrorism are estimated somewhere between $24 billion and $120 billion annually. These costs represent approximately 0.2% to 0.8% of the total GDP in the United States (McAfee 2013).

Cybercrimes against banks and other financial institutions can cost many hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information can cost developed economies billions of dollars—how many billions is an open question. These losses could be considered simply the cost of doing business, or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage (McAfee 2013).

Impact on the Environment

The impacts from cyber-attack are limited to infrastructure and people as highlighted in earlier sections. Therefore, there are no known impacts to the environment.

Cascading Impacts to Other Hazards

Cascading impacts that cyber-attacks may cause to other hazards include threats to the utilities reliant on power as well as the potable water supply; refer to Section 5.49 for discussion on Groundwater Contamination and additional details on the County's potable water supply.

Future Changes that May Impact Vulnerability

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

- Potential or projected development.
- Projected changes in population.
- Other identified conditions as relevant and appropriate, including the impacts of climate change.

Projected Development

As discussed in Section 4, areas targeted for future growth and development have been identified across Suffolk County. Any areas of growth could be potentially impacted by the cyber-attack hazard because the entire County is exposed and vulnerable. Additional development of structures or infrastructure which are reliant on computer systems could increase the County's risk to cyber-attack. Development of more structures using public power grids could also be affected by cyber-attacks and ultimately experience power outage. Therefore, understanding state requirements and recommendations may minimize risk for new development projects. For example, the New York Department of Financial Services issued a new set of cyber security regulations in 2017 for banks, lenders, mortgage companies, insurance companies, and service providers (NYS Department of Financial Services 2017). This regulation requires active protection against customer information by implementing a robust set of cybersecurity protocols including but not limited to the installation and use of a cybersecurity program, monitoring and testing of the selected program, and encryption of nonpublic information.

Projected Changes in Population

According to the Suffolk County Department of Economic Development and Planning's February 2017 Annual Report update, the population of the County is growing. The report indicates that slow population growth is expected to continue in the future, but it is important to note that the population is aging (Suffolk County 2017). An aging and growing population means that the number of persons vulnerable to cyber-attacks may increase for the County.

Climate Change

Because cyber-attacks are human-caused, no climate change impacts are associated with the cyber security hazard.

Change of Vulnerability Since the 2014 HMP

Cyber Security is a new hazard of concern for the 2020 Suffolk County HMP.