4.3.2 Cyber Attack

This section provides a profile and vulnerability assessment of the cyber attack hazard for the Dauphin County Hazard Mitigation Plan (HMP) update.

A cyber attack is the unlawful use of information technology, such as computer systems or telecommunications, to impact an individual or organization. This can include instances of cyber crime, such as using cyber attacks to steal or extort money from individuals or organizations or to cause property damage, as well as cyber terrorism. The term "cyber attack" often refers to an attack on information technology itself in a way that would radically disrupt networked services. For example, cyber attackers could disable networked emergency systems or hack into networks that house critical financial information. Cyber attacks can range from taking control of a host website to using networked resources to directly cause destruction and harm. A cyber attack is generally considered an act of cyber *terrorism* when the following conditions are present:

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

The Pennsylvania Department of Homeland Security defines the following types and methods of cyber attacks, as listed in the table below.

Table 4.3.2-1. Pennsylvania Department of Homeland Security Cyber Attack Definitions

Threat	Description
Botnet	A collection of computers subject to control by an outside party without the knowledge of the owners, using secretly installed software robots. The robots are spread by trojan horses and viruses. The botnets can be used to launch denial-of-service attacks and to transmit spam.
Card Skimming	The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit, or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases, or withdraw cash in the name of the account holder. Skimming can take place at an ATM, restaurants, axis, or other places where a user surrenders their card to an employee.
Denial-of-Service-Attack	Flooding the networks or servers of individuals or organizations with false data requests so they are unable to respond to requests from legitimate users.
Malicious Code	A code that can be used to attack a computer by spreading viruses, crashing networks, gathering intelligence, corrupting data, disturbing misinformation, and interfering with normal operations.
Pharming	The act of sending an email to a user falsely claiming to be an established legitimate enterprise to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information. The website is only used to steal the user's information.
Phishing	Using a fake email to trick individuals into revealing personal information, such as social security numbers, debit and credit card account numbers, and passwords for nefarious uses.
Spam	Unsolicited bulk email that may contain malicious software. Spam is now said to account for around 81 percent of all email traffic
Spear Phishing	Focuses on a single user or department within an organization, addressed from someone within the company on a position of trust and requesting information such as login IDs and passwords. Once hackers get this information, they can enter secured networks.
Spoofing	Make a message or transaction appear to come from a source other than the originator.
Spyware	Software that collects information without a user's knowledge and transfers it to a third party.
Swatting	The action or practice of making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address.
Trojan Horse	A destructive program that acts as a benign application. Unlike viruses, Trojan horses do not replicate themselves, but they can be just as destructive. One of the most common types is a program that claims to rid your computer of viruses but instead introduced viruses onto your computer.

Threat	Description
Virus	A program designed to degrade service, cause inexplicable symptoms, or damage networks.
Worm	Program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using the computer's resources and possibly shutting the system down. A worm, unlike a virus, has the capability to travel without human action and does not need to be attached to another file or program.

Source: Pennsylvania Department of Homeland Security (no date)

Cyber attackers can be difficult to identify because the internet provides a meeting place for individuals from various parts of the world. Individuals or groups planning a cyber attack can effectively communicate over long distances without delay (Pennsylvania Hazard Mitigation Plan 2018). There is wide disagreement about the extent of the existing threat by cyber attackers.

Cyber attacks can cause severe disruptions to transportation, public safety, and utility services, all of which (as critical infrastructure) are highly dependent on information technology. Cyber attacks can take many forms (as shown above), are unpredictable, and can occur without warning.

4.3.2.1 Location and Extent

Nationally, cyber security incidents or attacks have impacted residents, business and industry, and public utilities to varying degrees, and those threats would continue and likely expand in the future. Cyber attacks can occur anywhere within Dauphin County depending on an individual's or organization's agenda. Any processes that are networked and controlled by a computer are vulnerable to a cyber attack. Dauphin County government, its municipalities, and stakeholders such as academia, healthcare, National Guard, conservancies, residents, travelers, and business & industry (i.e., the whole community), are potential targets for cyber attacks. Cyber attackers can overtake websites, steal information, and alter the content that is presented to the public. Any vulnerability that could allow access to sensitive data or processes should be addressed and any possible measures taken to harden those resources to attack. Even with required cyber security protection, damage to or disruption of government and business operations can still occur and profoundly impact Dauphin County and its communities.

4.3.2.2 Range of Magnitude

The magnitude of cyber attacks has become more significant in recent years. Cyber attacks can greatly impact the whole community to varying degrees. The magnitude varies based upon which specific system is affected by an attack, the ability to preempt an attack, and an attack's effect on operations. As shown in Table 4.3.2-1, there are many forms of cyber attack, so the overall range of the magnitude of a cyber attack can vary from a skimmer collecting financial information from people who use a particular gas pump to a large-scale cyberterrorist attack that aims to disrupt government functions. Additionally, vulnerability to cyber attacks is greater where there are higher concentrations of people, businesses, and critical infrastructure. Also, as the City of Harrisburg serves as both the county seat and state capital, cyber attacks targeting people and systems in the City of Harrisburg could have cascading impacts affecting all areas of the county and/or Commonwealth.

In response to the growing cybersecurity threat, the National Institute of Standards and Technology developed the "Framework for Improving Critical Infrastructure Cybersecurity" in 2018. This document is described in Section 5 (Capability Assessment).

One worst-case scenario for a cyber attack event in Dauphin County would be a hacker illicitly accessing government systems, disrupting normal operations, intercepting calls, and emails, and gaining access to personal financial and other sensitive information. Another worse-case scenario would be a virus affecting a large portion of the computer population of the county, stealing credit card information, and causing millions of dollars in damage.

4.3.2.3 Past Occurrence

Residents, government, and other stakeholders are regularly impacted by cybersecurity incidents involving release of Personal Identifiable Information (PII) and other data, due to cybersecurity data breaches, such as Peekaboo, MGM Resorts, Walgreens, the Small Business Administration, and Marriott International, in 2020 alone. The majority of these incidents go unreported through standard emergency management channels and mechanisms.

The 2018 Pennsylvania HMP identified two cyber attacks that affected the whole Commonwealth. The first attack was an international cyber attack in 2017, and the second was a cyber incident in 2018 (PEMA 2018). The Dauphin County Department of Public Safety (DPS) was aware of two cyber attacks in the last five years- a ransomware attack in 2019 and an attack in 2020 that exploited a known Windows security vulnerability. Details are not provided here due to security concerns.

4.3.2.4 Future Occurrence

Members of the whole community within Dauphin County do not typically inform the county when a cyber attack or attempt has occurred. However, cyber attacks happen in one form or another on an almost daily basis, so the future occurrence of cyber attack in Dauphin County can be considered *highly likely,* as defined by the Risk Factor Methodology probability criteria (discussed in Section 4.4).

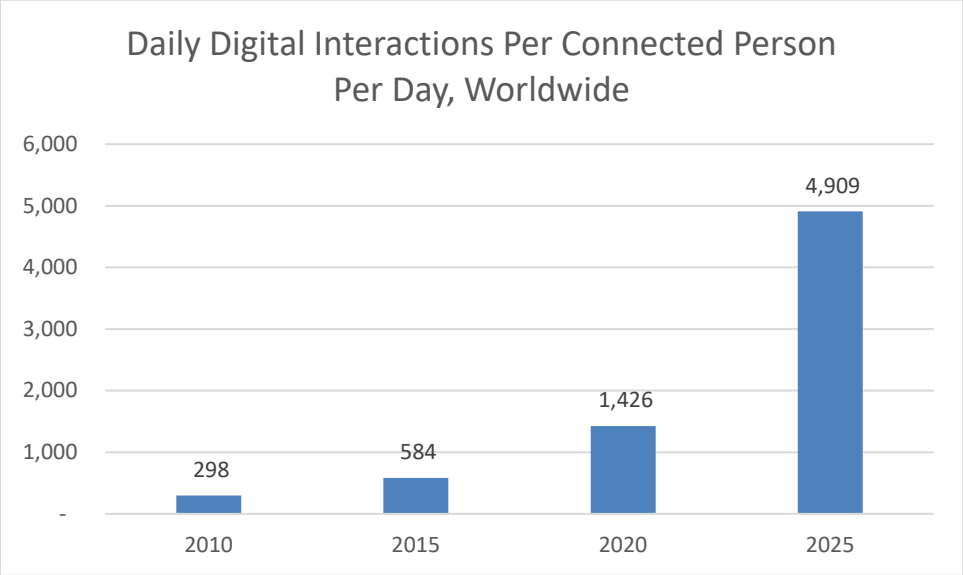
4.3.2.5 Vulnerability Assessment

To understand risk, the whole community must evaluate what assets are exposed or vulnerable in the area identified. The following sections discuss the potential impact of the cyber attack hazard in Dauphin County, including:

- Impact on (1) life, health, and safety; (2) general building stock; (3) critical facilities; (4) the economy; and (5) the environment
- Future growth and development
- Effect of climate change on vulnerability
- Additional data and next steps

As information technology evolves, so will the risk from cyber attacks. Cyber attacks today are largely based on existing operating system and network vulnerabilities. As the technology develops, cyber attackers will find new ways to exploit vulnerabilities. Vulnerabilities in the Internet of Things, including wearable devices (e.g. smart watches), smart homes and assistants (e.g., Alexa, Google Home, etc.), networked doorbells (e.g., Ring), etc. will increase the vulnerability to cyber attacks and provide new targets for malicious actors. The average person produces approximately 147 GB of data per day (Bulao 2021), and the average number of daily digital interactions per connected person worldwide is estimated to grow between 1,426 interactions in 2020 to 4,909 interactions in 2025 (Statista.com 2021), as shown in Figure 4.3.2-1. These statistics reflect the potential vulnerability to cyber attack across our society, including within Dauphin County.

Figure 4.3.2-1. Daily Digital Interactions Per Connected Person Per Day, Worldwide



Source: Statista.com 2021

Impact on Life, Health, and Safety

All 274,515 residents in Dauphin County are exposed to this hazard. Cyber attacks can impact the healthcare system (e.g., networked medical equipment may be vulnerable to hacking). Likewise, as autonomous vehicle technology progresses and autonomous vehicles become more common on Dauphin County's roadways, they are vulnerable to cyber attacks that could cause transportation accidents resulting in injuries or fatalities.

If the cyber attack targeted Pennsylvania'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., 274,515 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.

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 could be vulnerable to the secondary effects if the attack successfully caused a critical failure at that facility.

Impact on General Building Stock

Along with every home and business that is connected to the Internet, there are over 1,000 critical facilities in Dauphin County at risk of experiencing impacts from a cyber attack. A cyber attack can impact a building, 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. If a cyber attack targeted a fire suppression system, these structures would likely be at a higher risk for structural fire.

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 Commonwealth and an attack could disrupt power to thousands of Dauphin County 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. Cyber crimes 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 cyber security (McAfee 2013).

Individuals' personal information is also at risk. Commonly stolen personal information includes name, social security number, and drivers' license information. Because it is difficult to predict the particular target of cyber attack, 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 attack. Although all individuals in Dauphin County are vulnerable to an attack, certain types of attacks would impact specific segments of the population.

Given the proliferation of electronic commerce and the reliance on electronics, virtually all elements of Dauphin County'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 millions of dollars in tax revenue if these businesses were closed. Additionally, a disruption in Dauphin County'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 attack, it is safe to say that the impact would be great, thus the economy is vulnerable to cyber 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 attacks are estimated somewhere between $24 billion and $120 billion annually. These costs represent approximately 0.2 percent to 0.8 percent of the total GDP in the United States (McAfee 2013).

Cyber crimes 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 a cyber attack are usually limited to infrastructure and people, as highlighted in earlier sections. In the same way that people living near facilities that store or manufacture hazardous materials could be impacted by a cyber attack affecting those facilities, those attacks could also release hazardous materials into the environment.

Future Growth and Development

Areas targeted for potential future growth and development in the next 5 to 10 years have been identified across Dauphin County (further discussed in Section 2.4 of this HMP). Any areas of growth could be potentially impacted by the cyber attack hazard because Dauphin County is exposed and potentially vulnerable.

Effects of Climate Change on Vulnerability

Because cyber attack is a human-caused hazard, climate change is not anticipated to affect vulnerability associated with cyber attacks.

Additional Data and Next Steps

Any additional information regarding localized concerns and past impacts will be collected and analyzed for the HMP update. These data will be developed to support future revisions to the plan.