5.4.8 Cyber Attack

This section provides a profile and vulnerability assessment for the cyber attack hazard.

5.4.8.1 Hazard Profile

This section provides profile information including description, extent, location, previous occurrences and losses and the probability of future occurrences.

Description

A cyber attack is a malicious, intentional attempt to breach the information technology (IT) infrastructure of an individual or organization. Westchester County defines a cyber attack incident as an adverse event impacting one or more of the county's information assets. Examples include, but are not limited to, the following:

- Unauthorized use
- Denial of Service
- Malicious code
- Network system failures
- Application system failures
- Unauthorized disclosure or loss of information
- Information security breach
- Structured Query Language (SQL) Injection
- Other

Incidents can be the result of any of the following:

- Intentional and unintentional acts
- Actions of employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential policy violations
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing
- Other

The motives behind cyber attacks can vary widely, but according to Verizon (Verizon 2014), with input from over 50 organizations around the world, the top three motives in 2013 were

1. Financial
2. Espionage
3. Ideology/fun

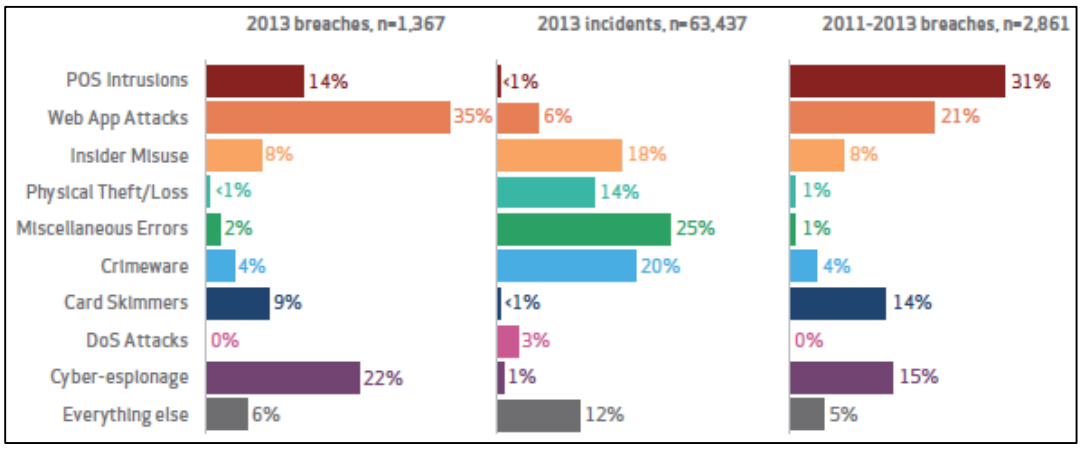
According to Verizon (Verizon 2014), 92% of over 100,000 cyber attacks over the last 10 years can be classified into nine different patterns, which are as shown for 2011-2013 in Figure 5.4.8-1. Figure 5.4.8-2 shows the percentage of all cyber attacks by pattern for several industries over that same time period.

Figure 5.4.8-2 shows that 34 percent of breaches in the public sector are Miscellaneous Errors – mistakes such as sending a sensitive document to the wrong person. Insider Misuse, Crimeware, and Theft/Loss are also significant sources of data breach; these three categories would constitute a cyber attack.

Westchester County's IT infrastructure includes the following components, which are potentially vulnerable to cyber attacks (2014 estimate).

- Nearly 5,900 network devices, including nearly 4,900 personal computers
- Over 600 servers
- Nearly 800 terabytes of data storage
- Over 6,000 phone instruments

Figure 5.4.8-1. Cyber Attack Patterns



Source: Verizon 2014

Figure 5.4.8-2. Cyber Attack Patterns by Industry

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

Source: Verizon 2014

Programs in Place to Reduce Impacts

Information Technology Systems

Mitigation of risk from cyber attacks is primarily handled by the County's Department of Information Technology with support from the County's security partners. The County's IT infrastructure includes the following components to reduce the impacts of cyber attacks:

- Firewall clusters
- Intrusion Prevention Systems (IPS) that alert on and block suspicious traffic

- Log collection platform that collects and analyzes logs from servers to detect potential threats
- Centrally managed security services that alert to potential threats within the IT environment, as well as emerging threats and vulnerabilities worldwide
- Endpoint protection (anti-virus/malware) on servers and PCs
- Data center security for enhanced monitoring & protection of critical servers
- Web filtering to block users from going to suspicious or known rogue websites
- Network traffic analysis
- NYS monthly Qualys scan report on public facing devices – Reporting on identified vulnerabilities
- Data Loss Prevention (DLP) for tracking Personally Identifiable Information (PII) or other sensitive data leaving the County's Network
- Daily and real-time reports from the County's security vendor on malware, viruses, phishing attacks, aggressive Secure Shell, and other intrusions based on the overall log collection apparatus.
- Ongoing security awareness program to educate and train county employees on cyber security best practices and policies

Response

Once an incident has been identified by the County, it is triaged to begin making decisions about how to address it. The County will then analyze computing devices, logs, and other files to identify the cause of the incident and to analyze and preserve evidence. It will then focus on identifying, removing and repairing the vulnerability that led to the incident, and thoroughly cleaning the system. After the cause of an incident has been removed or eradicated, and data or related information is restored, the County will confirm that all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced. The County will then decide to resume business operations, and will perform an after-action analysis. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meetings are held within one week of closing the incident.

Tabletop Exercise

In September 2014, Westchester County conducted a tabletop exercise to assess its cyber security capabilities. Participants included County departments, local municipalities, local utilities, and non-governmental organizations (NGO). The objectives of the exercises were as follows:

1. Examine government and partner organization capacity to manage the response to and short-term recovery from a non-traditional threat to the Westchester County area.
2. Examine government and partner organization continuity requirements and current preparedness posture.
3. Discuss multi-agency, multi-jurisdictional, and public-private sector communications and operational coordination structures and processes in the context of a no-notice incident with County-wide impacts and significant continuity implications.
4. Discuss key public messaging requirements and processes regarding an incident with widespread regional impacts, including electricity, communications and other lifeline infrastructure outages.
5. Identify gaps and challenges regarding the public-private sector response to and short-term recovery from an incident involving significant essential services disruptions/outages.

The exercise revealed strengths and areas for improvement regarding interagency coordination, communications, continuity planning, and cyber security planning.

Extent

When a cyber security incident occurs, Westchester County uses the following factors to evaluate its severity:

- Nature of the attack
- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people, agencies, or functions impacted
- Business considerations
- Public relations
- Effects on the County's entire IT enterprise

Cyber attacks may range from the infection of a single machine by a common computer virus to a large-scale, organized incident that cripples an organization or infrastructure.

Location

The cyber attack hazard is not geography-based. Attacks can originate from any computer to affect any other computer in the world. If a system is connected to the Internet or operating on a wireless frequency, it is susceptible to exploitation. Targets of cyber attacks can be individual computers, networks, organizations, business sectors, or governments. Financial institutions and retailers are often targeted to extract personal and financial data that can be used to steal money from individuals and banks.

Previous Occurrences and Losses

The County's security vendor produces a daily report that summarizes potential threats and intrusion attempts. Actions are taken by the Department of Information Technology to mitigate security risks presented in this report, by, for example, blocking IP address ranges, identifying vulnerable servers, performing scans as necessary, opening Help Desk tickets to scan/check machines, etc.

Losses can include loss of productivity, financial theft, and the exposure of secure information. No specific losses from cyber attacks that affected the County are available.

Probability of Future Events

As is the case for any large government organization, Westchester County will continue to be impacted and compelled to respond to cyber attacks in the future. The nature of these attacks is projected to evolve in sophistication over time. The County has taken a proactive position in its cyber security efforts and is expected to remain vigilant in its efforts to prevent attacks from occurring and/or disrupting business operations. The reality remains that many computers and networks in organizations of all sizes and industries around the U.S. will continue to suffer intrusion attempts on a daily basis from viruses and malware that are passed through web sites and emails.

5.4.8.2 Vulnerability Assessment

To understand risk, a community must evaluate what assets are exposed or vulnerable in the identified hazard area. For the cyber attack hazard, all of Westchester County is exposed to this hazard. Therefore, all assets in the County (population, structures, critical facilities and lifelines), as described in the County Profile (Section 4), are exposed and potentially vulnerable to a cyber attack. The following text evaluates and estimates the potential impact of the drought hazard on the County including:

- Overview of vulnerability
- Data and methodology used for the evaluation
- Impact on: (1) life, health and safety of residents, (2) general building stock, (3) critical facilities, (4) economy, and (5) future growth and development
- Effect of climate change on vulnerability
- Further data collections that will assist understanding this hazard over time

Overview of Vulnerability

The entire County is vulnerable to a cyber attack. Because it is difficult to predict the particular target of cyber terrorism, assessing vulnerability to the hazard is also difficult. All populations who directly use a computer or those receiving services from automated systems are vulnerable to cyber terrorism. Although all individuals in Westchester 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, individuals with medical needs would be impacted the greatest. These populations are most 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) 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.

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.

Data and Methodology

For this hazard, data was obtained from Westchester County and the Planning Committee.

Impact on Life, Health and Safety

Any individual in the County could be a victim of a cyber attack. If the attack targets infrastructure (such as the power grid) or individual life support systems in a healthcare facility, the effects of a cyber attack on life, health, and safety could be dire. Likewise, if a cyber attack affects the emergency response system, such as by rendering the 911 Center or the radio network inoperable, emergency services in the County could be hindered, which may result in increased injury or loss of life during emergency situations.

Impact on General Building Stock and Critical Facilities

Cyber attacks may affect structures if any critical electronic systems suffer service disruption. For instance, a cyber attack may cripple the electronic system that controls a cooling system or pressure system within critical infrastructure. This may result in physical damage to the structure from components overheating, or an explosion if pressure relief systems are rendered inoperable.

Impact on Economy

Economic impacts of cyber attacks could be severe, depending on the nature of the attack itself. Even simple malware that slows the performance of individual computers could result in lost business productivity. Any prolonged period of down time could significantly affect a business's financial performance. Retailers and financial institutions may be targeted to steal personal information so that the attacks' perpetrators can steal money from their victims, such as by opening credit cards with the stolen information.

Future Growth and Development

As discussed in Sections 4 and 9, areas targeted for future growth and development have been identified across Westchester County. Any areas of growth could be potentially impacted by the cyber attack hazard because the entire County is exposed and vulnerable. Please refer to the specific areas of development indicated in tabular form and/or on the hazard maps included in the jurisdictional annexes in Volume II, Section 9 of this plan.

Additional Data and Next Steps

For the Plan Update, any additional information regarding localized concerns and past impacts will be collected and analyzed. This data will be developed to support future revisions to the plan. Mitigation efforts could include building on existing New York State, Westchester County, and local efforts.