

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment

#### A. Hazard Profile

##### i. Hazard Description

While the broad reach of cyberspace has done much to improve communication, innovation, and information, its largely open and unregulated nature also leaves New York City vulnerable to cyber threats. A cyber incident, or the threat of such an event is an adverse event in an information system and/or network.

A cyber attack is an incident that is intentional and malicious in nature. An attack occurs when the digital infrastructure of a person or organization is compromised, often for financial or terror-related reasons. Such attacks vary in nature and are perpetrated using digital medium or, sometimes, social engineering, which targets human operators—as opposed to computers—as a primary vulnerability of a digital system. The growing dependence on digital infrastructure means that even a small incident at a targeted location may have widespread, damaging consequences.

Cyber attacks can take the form of data breaches, crippling viruses, or even physically damaging incidents. Generally, the hazard duration for such attacks last minutes to days, but large-scale events can last even longer.

Cyber attacks differ by motive, attack type, and perpetrator profile. Motivating factors for cyber attacks can vary tremendously; however most attacks fall into one of the following three categories: cyber crimes, hacktivism and cyber espionage. Hacktivism is the most common motivation for incidents affecting New York City, based on historical occurrences.

Six forms of cyber attacks are presented in Table 1 below:

Cyber Attacks	Attack Vectors	Description of Attack
Spoofing	Phishing	A person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage
Tampering	Defacement	Modification of data. Example: modification of website content or appearance can lead to propagation of misinformation
Repudiation	Insider	Challenging authenticity. Example: account compromise or unauthorized access to information technology—data, emails, or network access—leading to altering data integrity
Information Disclosure	Data Leak	The unintentional or intentional release of secure information—possibly private or confidential data—to an untrusted environment

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment

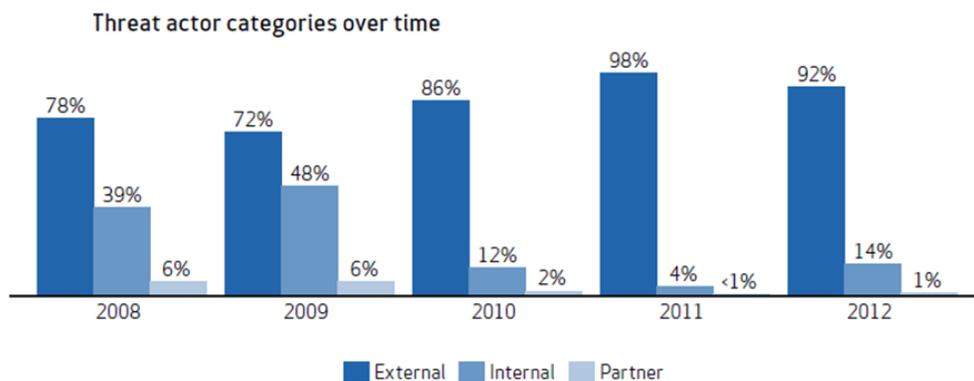
Cyber Attacks	Attack Vectors	Description of Attack
Denial of service	Distributed Denial of Service (DDoS)	An overwhelming number of false requests intended to prevent any legitimate service from functioning properly
Elevation of Privilege	Malicious code	Exploitation of a bug or design flaw, sometimes in an operating system, software application, database or website, which allows a user to gain higher levels of access to resources

**Table 1: Major Types of Cyber Attacks (Source: New York City Draft Cyber Incidents Response Protocol)**

Cyber attacks may be carried out by so-called external actors, internal actors, and partner actors (see Table 2). According to the Verizon 2013 Data Breach Investigation Report (DBIR), 92% of cyber attacks were perpetrated by external actors (see Figure 1).

Category	Category Description	Description of Attack
External	Outside of the victim organization	This category can be broken into subgroups: organized crime, state-affiliated, unaffiliated, unknown, activist, and former employees
Internal	Inside of the victim organization	In the past, 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
Partner	Third party sharing a business relationship with the victim	The least common of the three categories of attacks, this type of attack might be the result of, for example, a courier losing a device containing sensitive data

**Table 2: Perpetrator Categories for Cyber Attacks (Source: Verizon Wireless DBIR, 2013)**



**Figure 1: Threat Actor Categories 2008-2012 (Source: Verizon Wireless DBIR, 2013)**

### ii. Severity

There is currently no official index for measuring the severity of a cyber attack. However, the Gibson Index was created in February 2013 to serve as an open-source

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment

ranking system for the relative severity of cyber attacks. The Gibson Index ranges from 0 to 7, with 7 being the most severe class of attack.

- 0 – Little or no disruption
- 1 – Some small real-world consequences
- 2 – Clear malicious intent, resulting in longer outages
- 3 – Minor financial damages and moderate privacy implications
- 4 – Major financial damages and privacy implications
- 5 – Systematic, coordinated, broad penetration of a multitude of networks
- 6 – Attacks that manifest themselves in real-world, targeted, intentional damage
- 7 – Mass casualties from intentional, targeted efforts

#### iii. Probability

The probability of a cyber attack is difficult to calculate due to the unpredictability of human behavior.

#### iv. Location

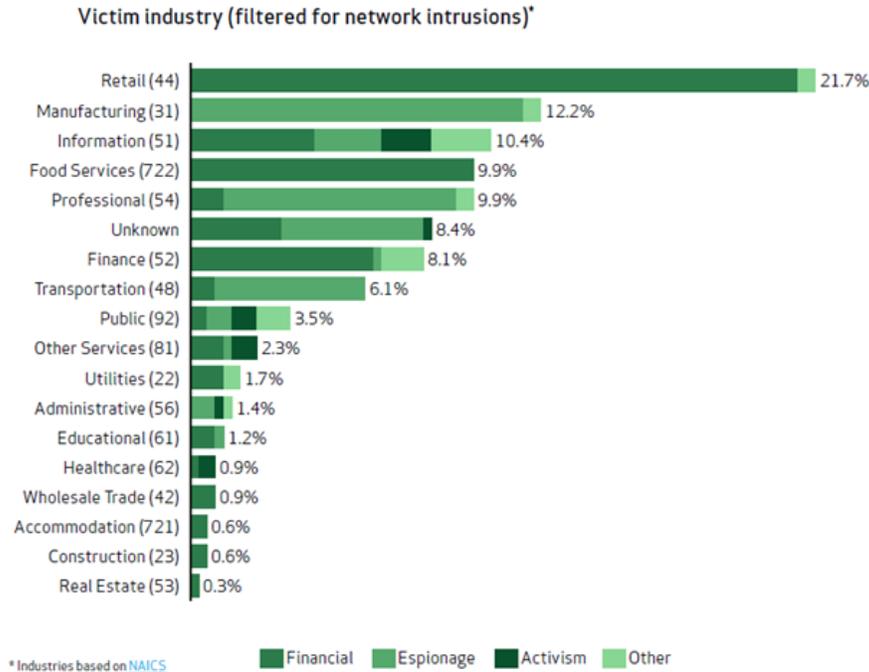
Unlike other hazards associated with specific geographic locations, the Internet is accessible remotely from any location. Attacks that affect New York City can originate from anywhere—even outside the city—adding an additional layer of complexity to protecting the city. The targets of these attacks can be very large corporations, governments, or even individuals—in fact, anything that is digitally connected is technically vulnerable. Specific target sectors that might result in citywide effects include:

- Financial centers
- Government buildings
- Media outlets
- Transportation authorities
- Power/Utilities companies
- Telecommunications networks

Figure 2, below, shows the breakdown of victim industries for cyber attacks in 2012, taken from the Verizon DBIR.

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment



**Figure 2: Victims of Cyber Attacks by Industry in 2012 (Source: Verizon DBIR, 2013)**

#### v. Historic Occurrences

There have been significant cyber attacks in New York City over the last few years, as indicated in Table 3, below.

Date	Category	Description
December 8, 2010	Denial of service	<ul style="list-style-type: none"> <li>Denial of service for Visa, MasterCard, and Paypal</li> </ul>
May 10, 2011	Information disclosure	<ul style="list-style-type: none"> <li>Data breach for 360,000 Citibank customers</li> <li>Cost of the breach was around \$22 million, with the hackers making \$2.7 million</li> </ul>
September 13, 2012	Denial of service	<ul style="list-style-type: none"> <li>New York Times hacked</li> </ul>
April 23, 2013	Tampering	<ul style="list-style-type: none"> <li>AP Twitter feed hacked</li> <li>A false message about explosions in the White House injuring President Obama is tweeted</li> <li>Attack causes Dow Jones industrial average to fall 128 points</li> <li>The White House is forced to reassure reporters that the president was all right and the report was false</li> </ul>

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment

Date	Category	Description
August 15, 2013	Denial of service	<ul style="list-style-type: none"><li>• CNN.com hacked by Syrian Electronic Army</li><li>• Deemed malicious external attack</li></ul>
August 15, 2013	Denial of service	<ul style="list-style-type: none"><li>• Syrian Electronic Army attack on the Washington Post website through a third-party service provided by a company called Outbrain</li></ul>
August 27, 2013	Denial of service	<ul style="list-style-type: none"><li>• Attack on New York Times and Twitter</li><li>• New York Times website was unavailable to readers due to an attack on the company's domain name registrar, considered more sophisticated than previous incidents</li><li>• New York Times website was inaccessible for over 10 hours</li><li>• Attack credited to Syrian Electronic Army</li><li>• Deemed malicious external attack</li></ul>

**Table 3: Significant Historic Cyber Incidents Affecting New York City 2010 to 2013**

### B. Vulnerability Assessment

#### i. Social Environment

The social environment is vulnerable to cyber attacks in a number of ways. Stolen personal information can destroy the financial standing of individuals. Additionally, cyber incidents can have a damaging effect on public trust in systems that are traditionally considered stable and secure—such as the nation's industrial, financial, and utility infrastructures. Cyber attacks can create fear and erode the public trust needed for private and public services to run successfully.

#### ii. Built Environment

A catastrophic cyber incident can have far-ranging effects on public and private infrastructure systems. Cyber attacks can cause physical damage if real assets or the end consumers are affected by service disruption. This might occur if cyber attacks target industries related to utilities, life support, transportation, human services, and telecommunications. In many cases, attacks on these systems initially will not be detected, and any malfunction will be thought to be system failure.

Cyber attacks can have extensive fiscal impacts. Companies and government services can lose large sums of unrecoverable revenue from site downtime and possible compromise of sensitive confidential data. Cyber incidents could result in the theft or modification of important data—including personal, agency, or corporate information—

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment

and the sabotage of critical processes, including the provision of basic services by government or private-sector entities.

#### iii. Natural Environment

While effects of cyber threats on the natural environment would be unlikely, they are conceivable. Like the effects on the built environment, the effects on the natural environment may come from a system failure that, for example, allows a release of hazardous materials or improper disposal of waste (see CBRN Hazard Analysis).

#### iv. Future Environment

Vulnerability to cyber attacks may change significantly in the future. As technology improves, security measures will improve, but cyber threat capabilities may also become equally sophisticated. The attack vectors, however, may stay the same. Since the threat of cyber attacks is increasing at a rapid rate, emphasis should be placed on preventative security measures.

## 16. CYBER THREATS

### Section III: Non-Natural Hazard Risk Assessment

#### Bibliography

Boyd, K., *The Gibson Index, Version 0.1.1*, February 2013,  
<http://www.gibsonindex.org/overview/> (last accessed December 11, 2013)

Department of Homeland Security Integrated Task Force, *Incentives Study Analytic Report*, June 12, 2013, Executive Order 13636: Improving Critical Infrastructure Cyber security, <https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf> (last accessed December 11, 2013)

Hernan, S.L., S. Lambert, T. Ostwald, and A. Shostack, "Uncover Security Design Flaws Using the STRIDE Approach", *MSDN Magazine*, November, 2006,  
<http://msdn.microsoft.com/en-us/magazine/cc163519.aspx> (last accessed December 11, 2013)

Transportation Sector Working Group August 2012, *Roadmap to Secure Control Systems in the Transportation Sector*, <http://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/TransportationRoadmap20120831.pdf> (last accessed December 11, 2013)

Verizon Data Breach Investigations, 2013, [www.verizonenterprise.com/DBIR/2013](http://www.verizonenterprise.com/DBIR/2013) (last accessed December 11, 2013)