



17. Cyber Threats

A. Hazard Profile

i. Hazard Description

The broad reach of cyberspace has done much to improve communication, innovation, and access to information. However, the largely open and unregulated nature of the Internet also leaves New York City vulnerable to cyber threats. These threats—whether a deliberate attack on an information system resulting in a data breach or the spread of a crippling virus, the threat of such an attack, or the accidental exposure of private information—can be extremely damaging. The growing dependence on digital interconnectivity means that even a small incident at a targeted location may have widespread, harmful consequences.

A cyber attack is a crime both intentional and malicious in nature. An attack compromises the digital infrastructure of a person or organization, often for financial or terror-related reasons. Such attacks vary in nature and are perpetrated using digital mediums or, sometimes, social engineering, which targets human operators—as opposed to computers—as a primary vulnerability of a digital system. Generally, attacks last minutes to days, but large-scale events—and their impacts—can last much longer.

Cyber attacks differ by motive, attack type and vector, and perpetrator profile.

Motives for cyber attacks can vary tremendously, ranging from the pursuit of financial gain—the primary motivation for what is commonly referred to as "cyber crimes"—to political or social aims. Hacktivism is the act of hacking, or breaking into a computer system, for a political or social purpose. It is the most common motivation for incidents affecting New York City, based on historical occurrences. Cyber espionage is the act of obtaining secrets without permission of the holder of the information, using methods on the Internet, networks, or individual computers.

Cyber attacks can also be grouped by attack type and

vector, or technique. As shown in Table 3.17.74, below, there are six attack types, each of which is carried out through specific vectors.

Table 3.17.74: Major Types of Cyber Attacks and Attack Vectors (Source: New York City Draft Cyber Incidents Response Protocol)

Attack Type	Attack Vectors	Description of Attack
Spoofting	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 leading to propagation of misinformation
Repudiation	Internal manipulation	Challenging authenticity. Example: account compromise or unauthorized access to information technology—data, emails, or network—leading to loss of data integrity
Information Disclosure	Data leak	The unintentional or intentional release of secure information—possibly private or confidential data—to an untrusted environment
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

Cyber attacks may be carried out by a variety of perpetrators. As shown in Table 3.17.75, perpetrators can be categorized as "external" actors (i.e. from outside the victim organization), "internal" actors (from within the victim organization), and "partner" actors (a third party sharing a business relationship with the victim). Most attacks are perpetrated by external actors. Ac-

17. CYBER THREATS

CHAPTER 3: RISK ASSESSMENT

According to the Verizon 2013 Data Breach Investigation Report (DBIR), 92% of cyber attacks in the country in 2012 were perpetrated by external actors, 14% were perpetrated by internal actors, and only 1% was the result of partner interaction (see Figure 3.17.105).

ii. Severity

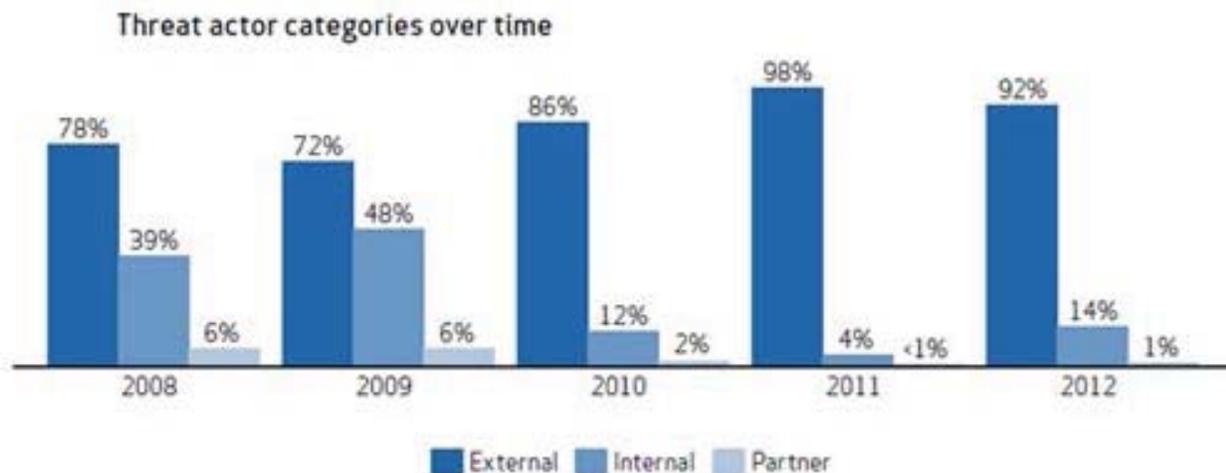
There is currently no official index for measuring the severity of a cyber attack. However, the Gibson Index, an open-source ranking system created in February 2013, is widely used in cyber threat analysis. The Gibson Index ranges from 0 to 7, as shown below, with 7 being the most severe class of attack.

- 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

Table 3.17.75: Perpetrator Categories for Cyber Attacks (Source: Verizon Wireless DBIR, 2013)

Category	Category Description	Description of Attack
External	Outside the victim organization	Attacks—which can be perpetrated by subgroups including organized crime, state-affiliated entities, unaffiliated individuals, activists, and former employees—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
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

Figure 3.17.105: Threat Actor Categories 2008 to 2012 (Source: Verizon Wireless DBIR, 2013)



iii. Probability

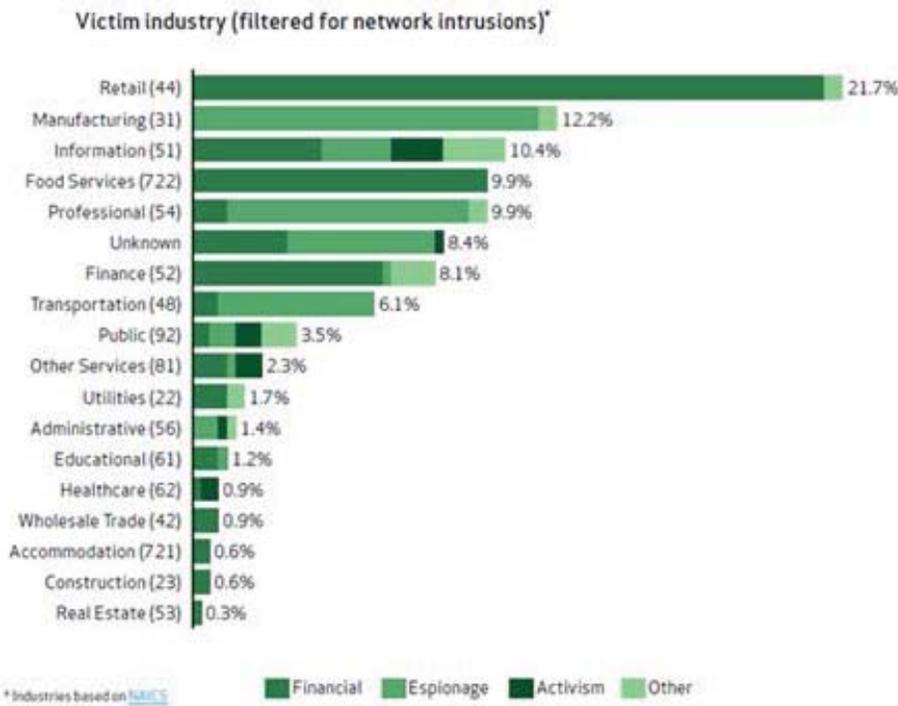
The probability of a cyber attack that will affect New York City is difficult to calculate due to the unpredictability of human behavior and the fact that the technology field continues to evolve quickly. While perpetrators of cyber attacks are becoming more sophisticated, companies and other users of digital technology are also getting smarter and learning to add layers of protection to systems and data.

nerable.

However, there are specific possible target sectors that might result in citywide effects. These include:

- Financial centers
- Government buildings
- Media outlets
- Transportation authorities

Figure 3.17.106: Victims of Cyber Attacks by Industry in 2012 (Source: Verizon DBIR, 2013)



- Power/utilities companies
- Telecommunications networks

iv. Location

Cyber threats differ from other hazards in that vulnerability to this hazard is unrelated to geographic location. The Internet is accessible remotely from all over the world. Attacks that affect New York City can originate from anywhere—including far outside the city—adding an additional layer of complexity to protecting the city. The targets of cyber attacks can be very large corporations, governments, or even individuals—in fact, anything that is digitally connected is technically vul-

Figure 3.17.106, below, shows the breakdown of victim industries for cyber attacks across the country in 2012, taken from the Verizon DBIR.

v. Historic Occurrences

There have been significant cyber attacks in New York City over the last few years, as indicated in Table 3.17.76, below.

Table 3.17.76: Significant Cyber Incidents Affecting New York City 2010 to 2013

Date	Category	Description
December 8, 2010	Denial of service	<ul style="list-style-type: none"> Denial of service for Visa, MasterCard, and Paypal
May 10, 2011	Information disclosure	<ul style="list-style-type: none"> Data breach for 360,000 Citibank customers Cost of the breach was around \$22 million, with the hackers making \$2.7 million
September 13, 2012	Denial of service	<ul style="list-style-type: none"> New York Times hacked
April 23, 2013	Tampering	<ul style="list-style-type: none"> AP Twitter feed hacked A false message about explosions in the White House injuring President Obama is tweeted Attack causes Dow Jones industrial average to fall 128 points The White House is forced to reassure reporters that the president was all right and the report was false
August 15, 2013	Denial of service	<ul style="list-style-type: none"> CNN.com hacked by Syrian Electronic Army Deemed malicious external attack
August 15, 2013	Denial of service	<ul style="list-style-type: none"> Syrian Electronic Army attack on the Washington Post website through a third-party service provided by a company called Outbrain
August 27, 2013	Denial of service	<ul style="list-style-type: none"> Attack on New York Times and Twitter New York Times website was unavailable to readers due to an attack on the company's domain name registrar—an incident considered more sophisticated than previous incidents New York Times website was inaccessible for over 10 hours Attack credited to Syrian Electronic Army Deemed malicious external attack

B. Vulnerability Assessment**i. Social Environment**

Cyber attacks can affect the population of New York City in a number of ways. Stolen personal information may 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. Cyber attacks may create fear and erode the public trust needed for private and public services to run successfully.

Cyber attacks can also have extensive economic 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—and the sabotage of critical processes, including the provision of basic services by government or private-sector entities.

ii. Built Environment

A cyber incident can have far-ranging effects on buildings and 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 it may be some time before it is known that system impairment or failure is the result of a cyber event.

iii. Natural Environment

While effects of cyber threats on the natural environment would be unlikely, they are conceivable. As with 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.

iv. Future Environment

Vulnerability to cyber attacks may change significantly

in the future. As technology evolves, more and more functions that were once grounded in the physical world go online, from building security to healthcare record-keeping. Security measures, too, will continue to improve, but, at the same time, cyber threat capabilities may also become increasingly sophisticated. The attack vectors, however, may stay the same. Cyber threats in various forms remain a genuine threat, and emphasis should be placed on preventative security measures.

17. CYBER THREATS

CHAPTER 3: 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 (last accessed December 11, 2013).