New York State Comptroller
THOMAS P. DiNAPOLI

Cyberattacks on New York's Critical Infrastructure

October 2023

Message from the Comptroller

October 2023

Information technology is a critical and irreplaceable element of our society. These systems are vital for our economy, public safety and national security, and they are more vulnerable than ever to exploitation.

Cyberattacks are a serious threat to America's critical infrastructure and have the potential to severely impact our day-to-day lives. These incidents often result in data breaches for companies and institutions that collect large amounts of personally identifiable data. Data breaches expose New Yorkers to invasions of privacy, the possibility of identity theft and other types of fraud. Even more troubling are incidents such as ransomware or distributed denial of service attacks that have the potential to shut down systems that we rely on for water, power, health care and other necessities.

In 2022, the FBI received 800,944 cybercrime complaints nationwide, an increase of 168 percent since 2016. Estimated losses from victims have also grown steadily, with $10.3 billion of losses in 2022 being seven times greater than in 2016. In New York, reported incidents grew by 53 percent between 2016 and 2022, with losses growing from $106.2 million to more than $775 million.

This report highlights the recent proliferation of cyberattacks, details the most common types, and discusses recent efforts to respond to and prevent such attacks. Finally, the report recommends a policy framework intended to help New York stay ahead of the threat presented by cyberattacks. The Office of the State Comptroller will continue to dedicate attention and resources to protecting New York residents and institutions from these attacks.

Thomas P. DiNapoli
State Comptroller

Table of Contents

Executive Summary

America’s critical infrastructure sectors are under near constant threat of cyberattacks, which have the potential to severely impact our day-to-day lives. Critical infrastructure refers to the systems and assets that are vital for the functioning of society, the economy and national security. This report focuses on the most common types of attacks: phishing, business email compromise, malware/ransomware, and corporate data breach.

Cyberattack Trends

According to data published by the Federal Bureau of Investigations’ Internet Crime Complaint Center (IC3), cyberattack complaints in New York increased 53 percent over six years, from 16,426 in 2016 to 25,112 in 2022. Attacks nationwide increased by 168 percent over the same period. Estimated losses in New York from cyberattacks in 2022 totaled over $775 million, while losses nationwide totaled $10.3 billion. New York had the fourth highest number of reported cybercrime victims in the nation in 2022. In New York State:

- From 2016 to 2022 complaints for Business Email Compromise (BEC) attacks grew the most, 91 percent.
- Relative to other states, New York had the third highest number of ransomware attacks (135) and corporate data breaches (238) in 2022, trailing only California and Texas for ransomware attacks and California and Florida for corporate data breaches.
- The three most attacked critical infrastructure sectors through ransomware and data breaches in New York were Healthcare and Public Health (9), Financial Services (8) and Commercial Facilities and Government Facilities were tied (7).
- Preliminary figures from the first 6 months of 2023 (through June) show that attacks on critical infrastructure in New York have already nearly doubled from 48 in all of 2022 to 83 in the first half of 2023.

Combatting the Threat

Reporting

The timely and accurate reporting of cyberattacks and data breaches is necessary to analyze trends and effectively prevent future attacks. In addition to data reported by the FBI through IC3, New York has several mechanisms for oversight and reporting of cyber incidents to sector-specific agencies. For instance, the New York State Information Security Breach and Notification Law, as amended by the New York State Shield Act, requires State entities, and any person or business in the State that maintains private information, to report any security breach that may compromise the confidentiality or integrity of private information and requires implementation of reasonable safeguards to protect personal information. The Securities and Exchange Commission has adopted new rules to enhance and standardize disclosures regarding cyber incidents, risk management and governance.[1]

Information Sharing and Coordination

Information sharing and collaboration among critical infrastructure owners, law enforcement, State and federal regulators, local governments and other public and private entities is necessary for the collective protection of critical infrastructure.

In June 2022, Governor Hochul appointed the State's first Chief Cyber Officer. Among other functions, the Chief Cyber Officer will lead the newly created Joint Security Operations Center (JSOC), which include agencies such as Office of Information Technology Services (ITS), the Division of Homeland Security and Emergency Services (DHSES) and the State Police. JSOC is to be the locus of coordination between federal, state and local governments and other organizations, and will spearhead implementation of the recently crafted State cybersecurity strategy.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations for the centralized reporting of incidents. The creation of a centralized repository of data breach reports from across the critical infrastructure sectors would also be beneficial to identifying new attack-vectors or exploits before they become widespread, and for coordinated response to emerging cyberthreats. Encompassing local governments in this database would be important.

Funding and Capacity Building

Under the Infrastructure Investment and Jobs Act (IIJA) of 2021, the federal government announced the State and Local Cybersecurity Grant Program (SLCGP), committing $1 billion over four years to help states, local governments, rural areas and territories address cybersecurity risks and improve their critical infrastructure resilience. By adopting the State's first cybersecurity strategy, New York will be able to access the federal grants.

The Enacted Fiscal Year 2023-2024 State Budget included $42.6 million to bolster cybersecurity across the State and included a new $500 million capital program to support upgrades to healthcare IT infrastructure. In addition, securing critical infrastructure requires sustained investment in network security and technological upgrades, as well as in developing in-house expertise to recognize, prevent, analyze, manage and remedy any threats.

Vigilance

The Office of the State Comptroller (OSC) works to help avoid cyberattacks by auditing and uncovering weaknesses in State, local government and school district cybersecurity systems. Audits by the Divisions of State Government Accountability and Local Government and School Accountability revealed dozens of ransomware attacks and other data breach incidents that compromised New York State agencies, counties, cities, towns and villages, hospitals and public-school systems, and have identified gaps in cybersecurity. Understanding and addressing these weaknesses can help New York State remain vigilant.

The Threat Landscape

Many aspects of our lives are now reliant on networked technology that is vulnerable to cyberattacks. Critical infrastructure refers to the systems and assets that are vital for the functioning of society, the economy and national security. They comprise a vast network of assets, systems and utilities that are necessary to maintain normalcy in daily life and retain vast amounts of personal identifiable data. Any incapacitation could have debilitating effects on our security, national economy, public health and safety, and exposure of their data could produce severe consequences for individuals. Appendix A includes a more complete description of the 16 critical infrastructure sectors, as well as information about their importance, functions and risks of attack.[2]

Figure 1
Critical Infrastructure Sectors

Chemical	Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services	Energy
Financial Services	Food and Agriculture	Government Facilities	Healthcare and Public Health
Information Technology	Nuclear Reactors, Materials, and Waste	Transportation	Water and Wastewater

Source: U.S. Cybersecurity & Infrastructure Security Agency (CISA)

Types of Cyberattacks on Critical Infrastructure

Cyberattacks can take several forms. Nationally, the most common are **phishing** attacks, in which fraudulent emails, text messages and phone calls that appear to come from a legitimate source make a request for sensitive information, such as login credentials or financial details, or to open malicious hyperlinks or attachments that can lead to unauthorized access to systems.[3] **Spear phishing** is an advanced form of phishing that targets an individual or specific organization, whereas regular phishing casts a wide net by sending out many emails, text messages, or messages through other online platforms in the hopes that people will reply.[4] Both regular phishing and spear phishing attacks are used to spread malware, such as ransomware.

Business Email Compromise (BEC), also known as email account compromise, is a form of spear phishing attack in which an attacker creates a fake email that looks like it is coming from a familiar and trusted source like a vendor, senior management or client. The user's trust in the sender is then leveraged to get them to click a link, open an attachment, or otherwise reveal confidential information or credentials. That information is then used to further compromise the target's systems or leveraged to defraud the target. In some instances, compromised email accounts are then used to send spear phishing attempts to the account's contacts.[5]

Malware attacks use malicious software that allow threat actors to gain unauthorized access, destroy or steal sensitive information and potentially control operating systems. **Ransomware attacks** are a type of malware attack involving software that encrypts the target's system and data, thereby preventing them from accessing it. The attackers then demand payment in return for the encryption key to decrypt the data and regain access to the systems. Ransomware attacks have been increasingly aimed at infrastructure sectors such as local governments, hospitals, banks and energy providers, leading to public safety concerns and significant financial losses.[6] (See text box for an example.)[7]

The 2021 ransomware attack on the Colonial Pipeline has been described by the U.S. Cybersecurity Infrastructure Security Agency as "a watershed moment" in cybersecurity. The Colonial Pipeline spans more than 5,500 miles from Texas to New York. On May 7, 2021, Colonial Pipeline experienced a ransomware attack on their billing systems. To prevent the spread of the attack, Colonial Pipeline shut down operations of the pipeline that carries 45 percent of fuel supplies for the East Coast, leading to fuel restrictions in 17 states. Colonial Pipeline paid the ransom to restore operation of the pipeline. Later, the U.S. Department of Justice recovered most of the ransom funds, but the incident spurred the adoption of policies to prevent future attacks.

Distributed Denial of Service (DDoS) floods a network/system with traffic in ways that increase computational or network demands, slowing down or interrupting service entirely. This traffic comes from many sources, typically a botnet, a vast network of compromised systems that can be called upon by an attacker to act in a coordinated manner.

Supply chain attacks insert malicious software or tampered hardware into the assets of suppliers, contractors and service providers. The 2020 attack on IT company SolarWinds is an example; a malware attack was delivered through SolarWinds servers during a software update affected the U.S. Treasury Department, the U.S. Department of Defense, and others.[8]

When it comes to supply chain threats, reliance on third-party vendors for software solutions has become increasingly necessary given the complexity of systems and reliance on technology to deliver services. Third-party software solutions are a part of the supply chain and may pose additional cybersecurity risks. One recent example is the recent mass exploitation of MOVEit file-transfer service attacks. (See text box.)[9]

MOVEit, a third-party vendor that offers secure software to transfer data and share files, is approved, accredited and meets numerous regulatory compliance requirements for several government agencies and regulated industries. Vulnerabilities in the software allowed attackers access to data across many public and private entities including the New York City Public Schools. As a result of the New York City Public Schools breach, approximately 45,000 students and 170,000 Department of Education Staff and third-party evaluators had personally identifiable information exposed including medical records, social security numbers, and student evaluations.

Many different types of cyberattacks are interconnected and can have cascading effects. For instance, successful attacks on communications networks and systems can disrupt emergency services, hindering response efforts during a crisis.

Examples of this include a 2019 ransomware attack on the City of Albany’s systems that impacted the police department’s systems and the 2021 ransomware attack on Albany, Saratoga and Rensselaer Counties’ 911 dispatch centers that partially disabled the dispatch computer systems.[10]

Similarly, targeting a financial institution can impact the entire financial services sector, potentially causing economic instability. Cyberattacks can also exploit interdependencies among critical infrastructure sectors. Disrupting the energy sector can impact transportation, telecommunications and healthcare. Disruptions in the financial services sector can affect supply chains and impact the availability of essential goods and services.

Key Trends in Cyberattacks

The FBI's Internet Crime Complaint Center (IC3) was established in 2000 as a central point for victims of cybercrime to report incidents and alert law enforcement to suspected internet crime activity. As the most accessible source of cybercrime data in the nation, the IC3 analyzes the information received through its website, categorizes the complaints and disseminates data to law enforcement and the public for investigation and intelligence purposes. [11] The IC3 data only represents what victims report to the IC3 and does not account for victim direct reporting to FBI field offices or other law enforcement agencies; therefore, the IC3 data is generally considered to be an indicator, but not a complete count.[12] Reporting requirements vary from state to state and from sector to sector, and even where reporting requirements exist, those crimes may or may not be reported to the IC3.

This report uses IC3 data to analyze trends in overall cybercrime as well as five major crime types that affect critical infrastructure sectors: Business Email Compromise, Corporate Data Breach, Ransomware, Malware and Phishing.[13]

Cybercrime Losses Have Spiked Since 2016

In 2022, the FBI received 800,944 cybercrime reports nationwide, an increase of 168 percent since 2016. 2022 losses were estimated to be nearly seven times the amount from 2016.[14]

2022 cybercrime incidents that were reported from New York increased 53 percent and losses grew 632 percent since 2016. New York had the fourth highest number of cybercrime victims in the nation in 2022. New York is a target-rich environment, with a large population and the presence of the New York Stock Exchange and other significant financial and economic institutions, large governmental institutions, and a high number of tech-sector companies.

Figure 2
Total Cybercrime Complaints and Losses, the Nation and New York, 2016 and 2022

	Complaints			**Losses (dollars in millions)**	
	US	**NY**		**US**	**NY**
2016	298,728	16,426		$ 1,500	$ 106.2
2022	800,944	25,112		$10,300	$ 777.1
Growth Rate:	**168%**	**53%**		**587%**	**632%**

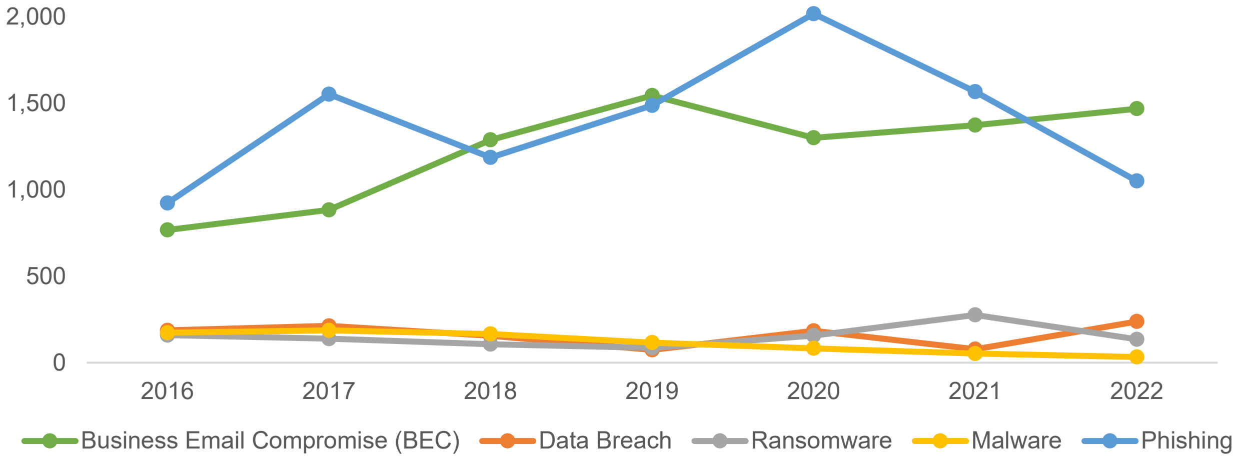
Source: IC3 Annual Reports, at https://www.ic3.gov/Home/AnnualReports.

Trends by Crime Type

Generalized phishing attempts are typically the most reported in the nation and have grown nationwide from 19,465 in 2016 to 300,497 in 2022. Reported phishing attempts saw a spike starting in 2019 that continued through the pandemic. In New York, the growth in phishing attempts was not as drastic as the nation (rising by 14 percent in the State from 2016 compared to 1,444 percent nationally).

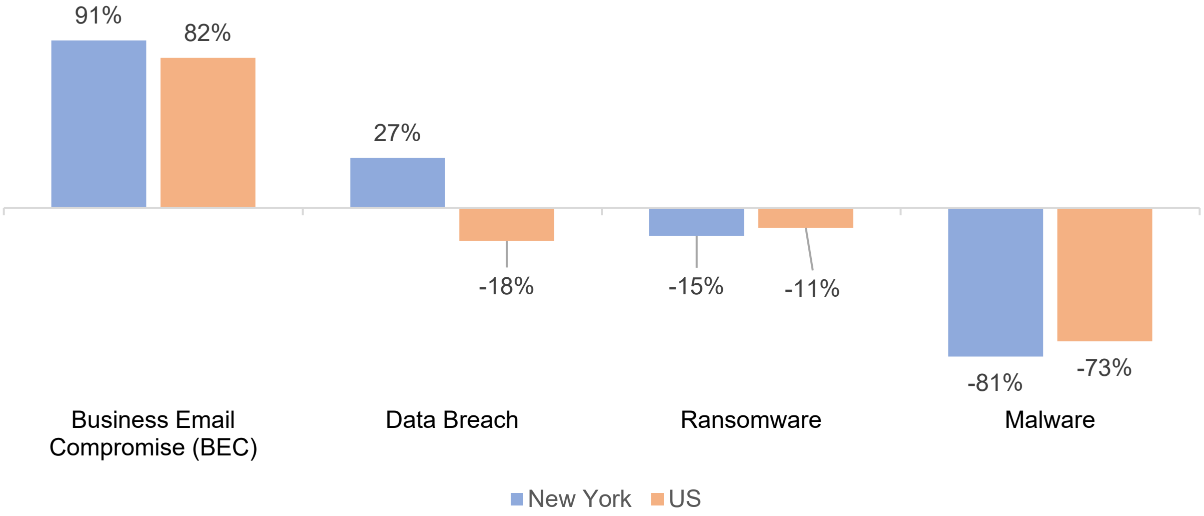
As shown in Figure 4, the number of business email compromise attacks in New York has almost doubled since 2016. While there are fewer incidents of data breach, ransomware and malware, the FBI considers each incident of a ransomware attack a serious threat to the public and the economy.[15] Incidents separately classified as "malware" have shown steady decreases over the past five years; however, this may be due to increased classification of complaints as other more specific crime types, like ransomware.

Figure 3
Number of Cybercrime Victims in New York, By Crime Type, 2016-2022



Source: IC3 Annual and State Reports, at https://www.ic3.gov/Home/AnnualReports.

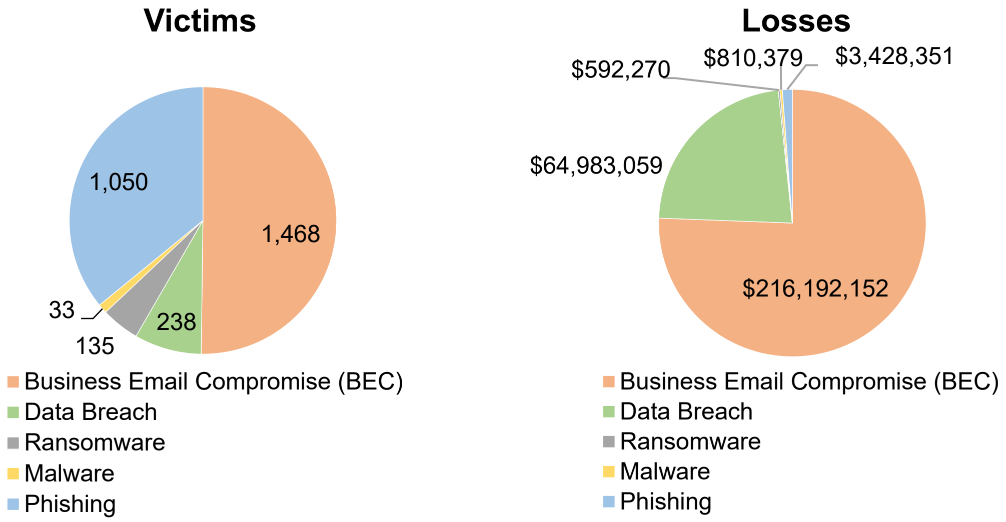
Figure 4
Percent Change in Select Cybercrimes, New York and the Nation, 2016-2022



Source: IC3 Annual and State Reports, at https://www.ic3.gov/Home/AnnualReports.

Of the five crime types analyzed, BEC attacks and corporate data breaches account for 98 percent of the total monetary losses for victims in New York in 2022. BEC made up half of all attacks and 76 percent of the losses. The number of BEC victims surpassed reported incidents of phishing in New York State in 2022, with BEC incidents rising to 1,468. Data Breaches made up only 8 percent of all five crime types analyzed, but resulted in 23 percent of losses. Phishing attacks totaled 36 percent of all attacks, but only 1 percent of the losses.

Figure 5
Cyberattack Victims in New York, By Crime Type, 2022



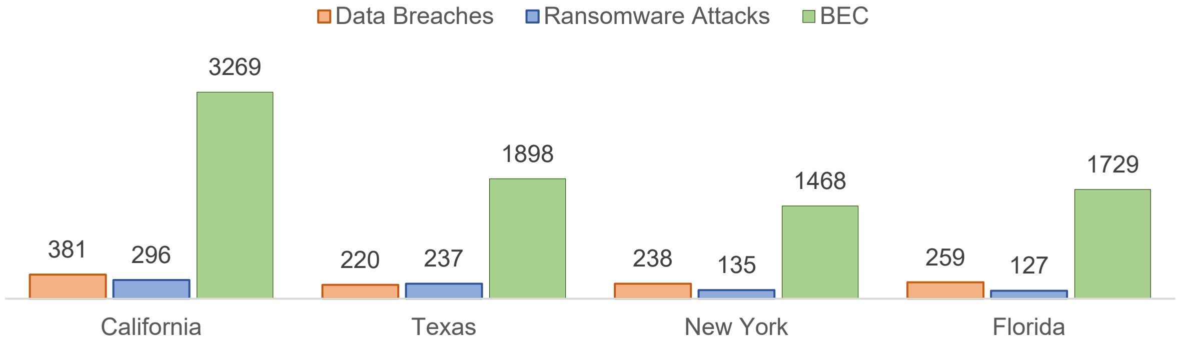
Source: IC3 State Reports, at https://www.ic3.gov/Home/AnnualReports.

State-to-State Trends in Ransomware and Data Breach

While most cybercrimes reported to the IC3 affect individuals, and the losses from them can be great, these types of cybercrime do not typically threaten critical infrastructure in a way that has potential for widespread economic and societal consequences. The most populous states have suffered the greatest number of ransomware attacks, data breaches, and BEC.

In 2022, New York had the third highest number of ransomware attacks (135) and corporate data breach incidents (238) in the nation. California ranked first for both crime types (ransomware: 296 and corporate data breach: 381). Texas ranked second for ransomware (237), while Florida was second highest in corporate data breaches (259). California ranked first in the nation for BEC (3,269), followed by Texas (1,898), Florida (1,729) and then New York with 1,468 attacks.

Figure 6
Number of BEC, Ransomware and Data Breach Victims in New York, California, Texas and Florida, 2022



Source: IC3 Annual Reports, at https://www.ic3.gov/Home/AnnualReports

Despite the high number of reported incidents in New York, other states reported greater estimated monetary losses from ransomware attacks in 2022. Illinois had the largest estimated losses at $4,309,000, followed by New Jersey ($3,681,954) and Kansas ($2,971,755). New York's estimated losses from ransomware were $592,270. For losses related to corporate data breach incidents, Alabama reportedly lost the most ($182,244,643), followed by New York ($64,983,059) and California ($46,132,944).

Cyberattacks on Critical Infrastructure Sectors

National Ransomware Attacks

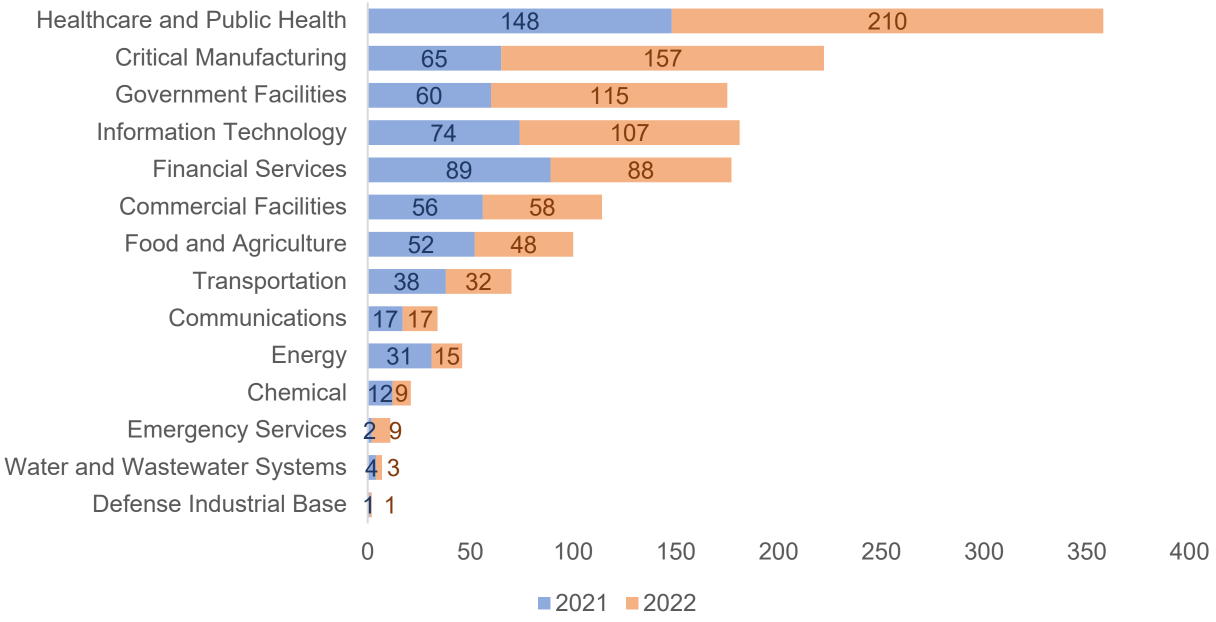
In June 2021, the IC3 began tracking the number of ransomware incidents reported by each critical infrastructure sector. Ransomware is a form of malware that encrypts and blocks access to computer files, systems, and networks. Attackers then demand payment to restore access. These attacks are particularly disruptive because they severely limit operations that rely on those systems or data and may also lead to critical data loss. While this might be disruptive to a business, when critical infrastructure is targeted by ransomware attacks, there is the potential that emergency response and lifesaving medical care could be impacted.[16]

In both 2021 and 2022, the IC3 reported victimization by a ransomware attack in 14 out of the 16 critical infrastructure sectors (excluding Dams and Nuclear Reactors, Materials and Waste Sectors). For the data collected in 2022, the top five sectors hit with ransomware attacks were:

1. Healthcare/Public Health (210 attacks)
2. Critical Manufacturing (157 attacks)
3. Government Facilities (115 attacks)
4. Information Technology (107 attacks)
5. Financial Services (88 attacks)

In 2022, the number of ransomware attacks in the Critical Manufacturing sector more than doubled from the prior year (65 to 157, or 142 percent), showing the highest increase in any sector in 2022. Ransomware attacks on Government Facilities almost doubled between 2021 and 2022, growing from 60 to 115. Ransomware attacks on the Financial Services industry remained high in 2022. Ransomware attacks on the Information Technology sector increased by 33 (45 percent) over 2021.

Figure 7
Infrastructure Sectors Victimized by Ransomware in the Nation, 2021-2022



Source: IC3 Annual Reports, at https://www.ic3.gov/Home/AnnualReports.

State-Level Ransomware Attacks and Data Breaches

According to supplemental state-level data provided by the IC3 that includes only ransomware and data breach attacks, cyberattacks occurred in 12 out of 16 critical infrastructure sectors in New York in 2022 (attacks were not reported in Dams, Defense Industrial Base, Emergency Services and Nuclear Reactors, Materials and Waste sectors). The Healthcare sector reported the most cyberattacks (9), followed by Financial Services (8), Commercial Facilities and Governmental Facilities (both 7), and Critical Manufacturing industry reported 6 attacks in 2022.

Attacks on local governments in recent years have had troubling consequences. For instance, in 2019 a ransomware attack on the Syracuse City School District froze the district out of its own systems, crippling the website, email system, phones, and back-end functions like payroll and student management.[17]

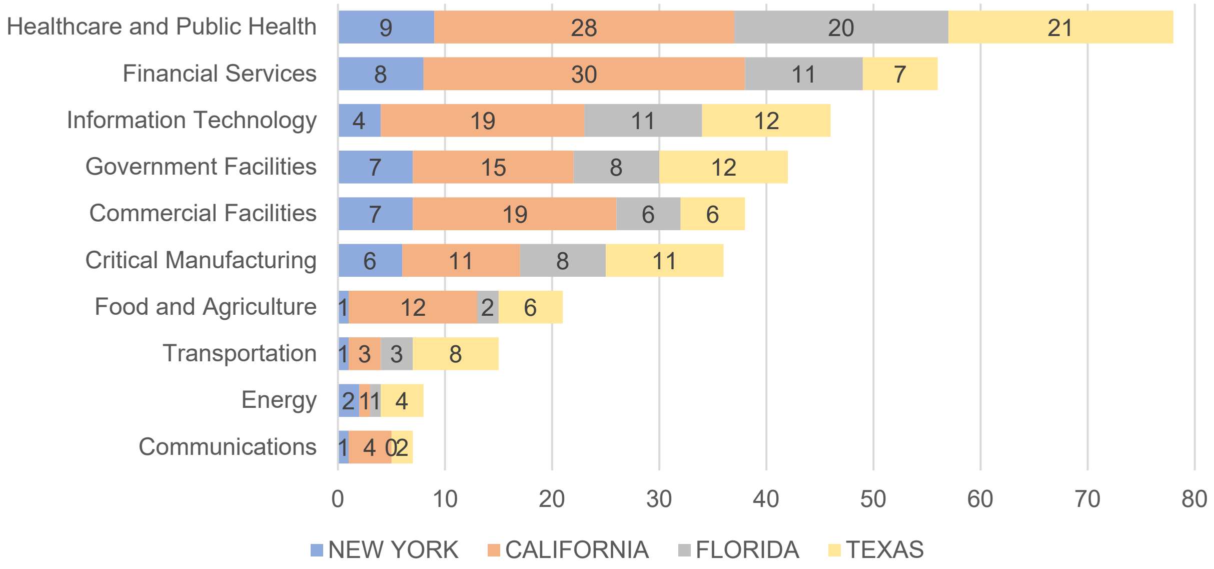
Other attacks on local governments have had far-reaching impacts. The September 8th, 2022 ransomware attack on Suffolk County required the County to disable computer systems including 911 dispatch and the Department of Motor Vehicles systems, and move many of the County's functions including that of the 911 dispatch center and the police department back to pen and paper for months. A powerful example of the impact of a cyberattack, the incident highlights the potential risk to State systems that linked local government systems could pose, particularly in the absence of zero-trust authentication policies.[18]

Ransomware attacks on the healthcare sector are particularly dangerous because in addition to exposing patients personal and personally identifiable data in data breaches, these attacks risk affecting patient care and outcomes. (See text box for more information.)[19]

When compared to the three other most populated states in the nation, New York suffered fewer attacks. California reported the most attacks on infrastructure sectors in 2022 (142), followed by Texas (90) and Florida (71). Figure 8 shows a state-to-state comparison for the infrastructure sectors that have suffered the most attacks nationwide.

In 2022, an attack on One Brooklyn Health, a hospital group that includes Interfaith Medical Center, Brookdale Hospital Medical Center, and Kingsbrook Jewish Medical Center, forced doctors and nurses to provide patient care using pen and paper, and limited access to patients' health records that were stored electronically for weeks. The attack also exposed the personal data of an estimated 235,000 patients according to a class action lawsuit filed on behalf of the victims.

Figure 8
Ransomware and Data Breach Attacks on Select Infrastructure Sectors in New York, California, Florida and Texas, 2022

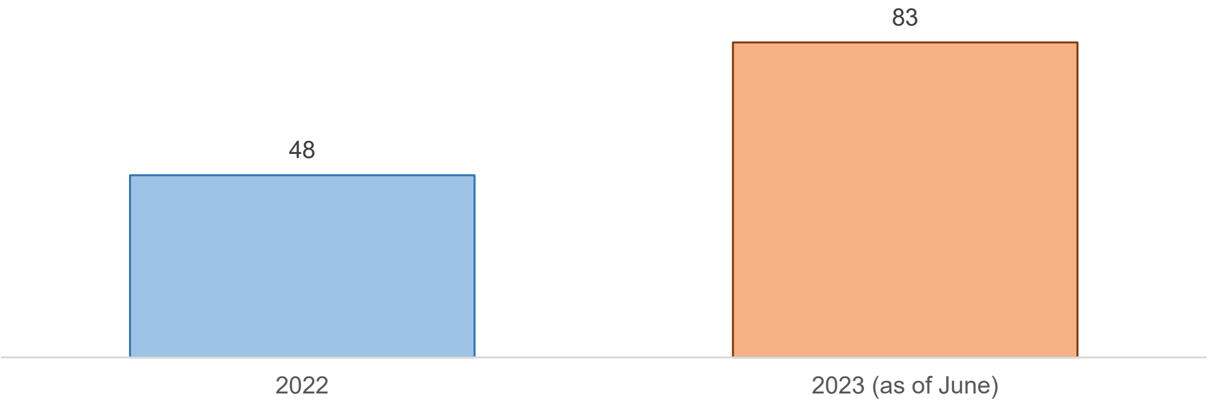


Note: The Defense Industrial Base, Dams, and Nuclear Reactors, Materials and Waste Sectors did not report cyberattacks in these four states in 2022. Figure 8 also omits Chemical, Emergency Services, and Waste and Wastewater Sectors. In 2022, New York suffered one attack in Water and Wastewater and one attack in Chemical sectors.

Source: IC3 Supplemental Data

Preliminary figures from the first six months of 2023 show that the number of cyberattacks on critical infrastructure in New York State has nearly doubled from the total amount in all of 2022. As of June 2023, the Information Technology Sector has seen the largest jump since last year, with reported attacks already rising from 4 in 2022 to 14 so far in 2023. The Healthcare and Financial Services industries have also seen a large volume of cyberattacks in the first half of 2023 with 16 and 15 each, respectively; already doubling reports from last year.

Figure 9
Cyberattacks on Critical Infrastructure in New York, 2022 and from January to June 2023



Source: IC3 Supplemental Data

Combatting the Threat

The protection of critical infrastructure is the responsibility of multiple layers of overlapping agencies, organizations, and regulatory authorities. The requirements for effective cybersecurity are frequently established by regulatory bodies at the State and federal level. Law enforcement, primarily on the federal and State level, investigate crimes after they occur and issue alerts and warnings about emerging threats or patterns of attacks. Preventing cyberattacks typically falls to other specialized government agencies, as well as the owners of critical infrastructure (public and private).

Reporting Requirements

The timely and accurate reporting of cyberattacks and data breaches is important. Without comprehensive reporting and tracking of incidents, the entities charged with protecting our critical infrastructure cannot respond, investigate, protect or notify affected parties.

In New York, there are several mechanisms for oversight and reporting of cyber incidents to sector-specific agencies. The broadest is the New York State Information Security Breach and Notification Law and the New York State Shield Act, State entities, that requires any person or business in the State that maintains private information must report any security breach that may compromise the confidentiality or integrity of private information and implement reasonable safeguards to protect personal information.[20] While the State Technology Law requires local governments to notify individuals when there is a security breach that compromises private or personal information,[21] there is currently no requirement for local governments to report incidents to a centralized State agency. For more information on New York State's additional cyberattack reporting requirements, please refer to Appendix C.

In July 2023, the U.S. Securities and Exchange Commission (SEC) adopted final rules requiring publicly traded companies and foreign private investors who are registered with the SEC to report cybersecurity incidents within four business days after they determine that an incident is "material." SEC registrants are also required to disclose on an annual basis information regarding their cybersecurity risk management, strategy, and governance procedures.[22]

In March, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was passed by the federal government and requires CISA to develop regulations on cybersecurity reporting. Once those regulations are adopted, covered entities in defined critical infrastructure sectors will be required to report cybersecurity incidents within 72 hours and to report a ransomware payment within 24 hours.[23] Rules are in the process of being made on what is a covered entity, what qualifies as an incident and how incidents will be reported.[24]

Information Sharing and Coordination

Robust reporting requirements are necessary for the protection of critical infrastructure, but the value of the information collected through data breach reporting is limited if that information is siloed. Information sharing and collaboration among critical infrastructure owners, law enforcement, State and federal regulators, local governments, and other public and private entities is necessary for the collective protection of critical infrastructure.

Federal

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) serves as the lead federal agency for preventing attacks and executing the nation's cybersecurity strategy. It provides cyber-threat information sharing, vulnerability assessments and incident response coordination among government agencies and private sector partners. [25] Through CISA and other policy directives, the federal government works to develop and enhance cybersecurity frameworks that provide guidance, best practices and standards for organizations to manage cyber risks effectively and improve their resilience against cyberattacks.

The National Security Agency and the FBI's Cyber Crime division also play important roles, with the former supporting the development of secure technologies, conducting research, and providing tools and guidance[26] and the latter spearheading collaborative law enforcement efforts and investigating and apprehending cyber threat actors. [27]

In March 2023, the Biden Administration released its National Cybersecurity Strategy, followed by an Implementation Plan for the Strategy in July.[28] The White House Strategy recommends harmonizing cybersecurity regulations in the critical sectors, improved information sharing and coordinated incident response among the government and private sector, the need to expand the cybersecurity workforce and invest in cybersecurity technology research to keep up with new and emerging cyberattack vectors. The Introduction in the Plan recognizes that it "is a living document" that will be updated annually as the cyber threat landscape changes. DHS also publishes its own five-year Cybersecurity Strategy.[29]

New York

In New York the Office of Information Technology Services (ITS), the Division of Homeland Security and Emergency Services (DHSES) and the State Police work together to prevent and respond to cyberattacks. ITS is responsible for establishing standard security requirements and ensuring the reliability of the cybersecurity infrastructure for the State's Executive agencies.

DHSES coordinates the State's overall cybersecurity posture with other State agencies, local governments and private sector partners to assess cyber risks, facilitate cyber incident response, and promote cybersecurity awareness and training initiatives.[30] DHSES is not a law enforcement agency but works with the New York State Police and the New York State Intelligence Center to receive and disseminate intelligence on reports of cyber incidents.[31] DHSES includes a Critical Infrastructure Protection Unit and a Cyber Incident Response Team within its Office of Counter Terrorism, both of which provide support to the State's non-Executive agencies, local governments, and public authorities (including over 2,800 entities not covered by ITS support services).[32]

In 2022, Governor Hochul appointed a Chief Cyber Officer for the State to lead cross-agency efforts to combat cyber threats and improve the State's critical infrastructure assets. Among other functions, the Chief Cyber Officer will lead the newly created Joint Security Operations Center (JSOC), a multi-agency cybersecurity coordination hub linking New York State, New

York City, local and regional governments, critical infrastructure stakeholders, and federal partners for information sharing, cyber threat detection and incident response.

On August 9, 2023, the Executive released the first statewide cybersecurity strategy to meet the cybersecurity plan requirement to access State and Local Cybersecurity Grant Program funding. The strategy aims to coordinate the efforts of state, county, and local governments with the Federal government and private industry, to expand the scope of regulations, requirements, and recommendations to protect critical infrastructure, and to provide advice and guidance to empower New Yorkers to take part in their own security.

The statewide strategy focuses on five areas:

- Operating State Government networks securely and resiliently by modernizing state networks and systems according to zero-trust principles and implementing multi-factor authentication;
- Increased collaboration and support among State and local governments and federal agencies on cybercrime prevention and response;
- Development of the State's cybersecurity workforce;
- Regulating critical infrastructure sectors to heighten their cyber defenses; and
- Educating New Yorkers about cybersecurity by communicating guidance and advice to help them know what threats are present and how to protect themselves.

The strategy emphasized the importance of protecting local government systems, which are often linked to State systems. The exploitation of vulnerable local systems poses a security threat to linked State systems. It also relies on increased investment and expansion of the JSOC as a centralized locus to assess threats, issue guidance, and coordinate responses to cyber threats. It clarifies agency roles and responsibilities, and outlines a unified approach to protect critical infrastructure, networks, and data.

In addition to these efforts, the New York State Department of Financial Services and the State Education Department have implemented regulatory programs to monitor the cybersecurity health of the critical sectors they oversee within the State. The New York State Office of the Attorney General (OAG) Internet Bureau investigates and prosecutes cases involving data breaches, identity theft, fraud and other cyber offenses, and nonprofit organizations such as the Center for Internet Security (CIS) also partner with government agencies to improve information sharing through CIS's Multi-State Information Sharing & Analysis Center. CIS also offers its members incident response and remediation support, as well as advisories that provide information on improving cyber security.[33]

Funding and Capacity Building

As part of the Infrastructure Investment and Jobs Act (IIJA) of 2021, the federal government announced the State and Local Cybersecurity Grant Program (SLCGP), committing $1 billion over four years to help states, local governments, rural areas, and territories address cybersecurity risks and improve their critical infrastructure resilience. Each state or territory that applies must establish a Cybersecurity Planning Committee and a Cybersecurity Plan.

Thereafter, the state or territory must pass through at least 80 percent of the funds awarded to local governments, including at least 25 percent of funds to rural areas. The SLCGP provides funding for local governments to modernize their networks against future cyberattacks, protecting the services these governments provide to their communities.

The Enacted Fiscal Year 2023-2024 State Budget included $42.6 million to expand the State Police Cyber Analysis Unit and create a new specialized Industrial Control System (ICS) Assessment Team within DHSES. This funding is aimed at providing new hardware and software cybersecurity tools, and additional cyber personnel, for State and local government systems. It also included a new $500 million capital program to support upgrades to healthcare IT infrastructure. This builds on last year's $61.9 million investment for cybersecurity in the State Budget, adding enhancements to statewide services and providing funding to help local governments bolster their cyber defenses.

Vigilance

The Office of the State Comptroller (OSC) works to help avoid cyberattacks by auditing and uncovering weaknesses in State, local government and school district cybersecurity systems, and making recommendations intended to help protect against more sophisticated future cyberattacks.

OSC's Division of State Government Accountability (SGA)

SGA has found several common technical weaknesses and risks across its audits, such as: entities' misunderstanding of security risks, unsupported applications, unknown data on systems, poor access controls and a lack of monitoring of changes to systems, among others. In conjunction with the public release of the audit report, SGA also issues a confidential report to entity officials, enabling them to begin corrective actions immediately. In addition, SGA performs a follow-up review one year later for each IT audit, to assess whether the entity has made all the necessary changes previously recommended to strengthen their networks.

In 2021, SGA researched the number of entities in the State that were affected by cyberattacks over the preceding six years, revealing dozens of ransomware attacks and other data breach incidents that compromised New York State agencies, counties, cities, villages and towns, as well as hospitals and public-school systems. Law enforcement agencies and county 911 systems were affected, critical government services and transportation were temporarily shut down in several municipalities, and social security numbers of individuals were revealed in some instances.[34]

Following this research, SGA conducted several audits targeted at improving cybersecurity for the State's critical infrastructure. Most recently, SGA reviewed the State Department of Health's (DOH) regulatory oversight of public drinking water supplies. The audit revealed that nearly 95 percent of all New Yorkers at some point in their day-to-day activities use water from public water supply systems in the State. In June 2023, SGA published its report,[35] finding community water systems need to update and bolster their Water Supply Emergency Plans, which include a requirement to conduct a Cybersecurity Vulnerability Assessment.[36]

In another recent audit, SGA reviewed how the State Education Department (SED) oversees school districts' protection of student data privacy.[37] The report noted how the pandemic's transition to technology-based remote learning resulted in heightened cybersecurity threats, making it more important than ever to ensure that schools have secure systems that protect the privacy of students' data.[38] The audit recommended, among other things, that SED develop and implement new controls to improve the reporting of data breaches by school districts, and complete a full data classification of its information to ensure that student data has appropriate security controls. Since that time, SED has begun to address the issues identified and has taken steps to implement SGA's recommendations.

In 2021, SGA conducted an audit of DHSES Cyber Incident Response Team (CIRT). The audit found that between May 2018 and December 2020, CIRT responded to 122 cyberattacks statewide. To more effectively measure whether CIRT is achieving its mission, the audit recommended that DHSES develop specific quantifiable goals to evaluate the effectiveness of its response services and information sharing on cyber incidents. SGA also recommended that CIRT begin proactive outreach to the entities it assists to provide more training opportunities and risk assessments to address cybersecurity needs before cyberattacks occur.[39] Since SGA's final report was issued, DHSES CIRT has implemented a more proactive risk-based approach to providing outreach to the entities it serves, including using factors such as history of past incidents, the population an entity serves, sensitivity of data assets, and the critical nature of the services an entity provides.[40]

In addition to these most recent initiatives, SGA has completed audits and made recommendations on other cybersecurity-related issues, such as:

- Replacement and remediation of the State Department of Labor's Unemployment Insurance system following a significant uptick in fraudulent claims during the pandemic.[41]
- Recommending that the State Office of Information Technology Services (ITS) implement additional security controls according to ITS policies and standards, to ensure appropriate management of the State's Active Directory domains.[42]
- Determining that the State Board of Elections has effectively used federal funding to enhance the cybersecurity of the State's election technology and infrastructure.[43]
- Recommending that the State University's Upstate Medical Center improve controls over improper user access to confidential patient information.[44]

OSC's Division of Local Government and School Accountability (LGSA)

From January 2019 through July 2023, LGSA released 191 IT-related audits, reporting on 2,366 IT findings, largely related to breakdowns or gaps in basic cybersecurity components for local governments and schools. In addition to conducting risk assessments and audits, and issuing guidance publications and research reports, LGSA provides free cybersecurity training and technical assistance to the local governments and school districts it serves. For example, a series of Local Government Management Guides provide information, resources, and best practices on cyber-related topics such as:

- Information Technology Governance (focused on strengthening IT systems and controls, and contains a cybersecurity self-assessment tool designed to help boards and officials assess their cybersecurity environment and recovery readiness);
- Ransomware (discussing how to prevent and respond effectively in the event of a ransomware attack); and
- Industrial Control Systems (ICS) Cybersecurity (these are systems that gather information on an industrial process and modify or manage the process to achieve a desired result. Most of the nation’s critical infrastructure is run with help from ICS). [45]

Conclusion

Critical infrastructure is indispensable to the functioning of modern society, and understanding each sector’s significance, functions and associated risks is essential for effective preparedness, resilience and response efforts. Securing this infrastructure from cyberattacks will require sustained investment, coordination and vigilance.

Sustained Investment

The State is taking actions to bolster its own funding and craft and implement a statewide cybersecurity strategy, which will also allow it to access federal funds. Sustained investment in the security of the networks, IT systems, and software that critical infrastructure relies on will be necessary and should be considered as a part of the costs of future technological upgrades. In addition, securing critical infrastructure requires sustained development of in-house expertise to recognize, prevent, analyze, manage and remedy any threats. Given the existing challenges in recruitment and retention of public employees, growing the State’s public sector cybersecurity workforce will not be easy, but must be identified as a priority.

Coordination

The statewide cybersecurity strategy serves as a first step for the coordination of security of critical infrastructure. Implementation of the strategy, however, will not be without challenges. The strategy hinges on coordination and collaboration between partners and stakeholders that in the past have been far more siloed.

Reporting and transparency of data breaches are crucial to identifying new threats before they become widespread, and for coordinated response to emerging cyber-threats. Informing and advising victims of data breach on the actions they can take to limit the threat is also crucial to limiting the fallout from a cyberattack. Current data breach reporting requirements vary depending on what entity was breached, and while there are several State agencies and offices responsible for receiving notifications of data breaches, there is no centralized repository of the reports.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations for the centralized reporting of incidents. The creation of a centralized repository of data breach reports from across the critical infrastructure sectors would be beneficial to identifying new attack-vectors or exploits before they become widespread, and for coordinated response to emerging cyberthreats. Encompassing local governments in this database would be important.

Vigilance

As technologies become more advanced, those who seek to exploit technological vulnerabilities also evolve. Protecting against this threat requires committing to a path of constant innovation to proactively protect and remain ahead of the curve. OSC’s cybersecurity audits have revealed that State agencies tend to address cybersecurity issues reactively and lack sufficient proactive planning and prevention strategies. The audits have recommended State agencies do more frequent vulnerability assessments and proactively establish standard cybersecurity policies – both for their own systems as well as the systems they are responsible for overseeing. In addition, these audits have frequently recommended that State agencies establish and regularly update emergency plans, including plans for cyberattacks, and improve controls over access to confidential information often held by government agencies, school districts and healthcare providers.

For local governments, audit findings were commonly related to the need for updated cybersecurity training and procedures to appropriately restrict IT user access to personal, private and sensitive information and to ensure that employees and third-party contractors understand procedures that need to be followed. OSC has also recommended IT contingency planning for possible cyber disruptions, which will help prepare personnel for any needed actions in the event of an actual disruption and could significantly reduce the resulting impact.

Appendix A

Critical Infrastructure Sectors: Importance, Functions and Risks of Attack

1. **Chemical Sector:** The chemical sector encompasses facilities that produce, distribute and store various chemicals. It provides vital resources for manufacturing, agriculture, pharmaceuticals and other industries. Most chemical facilities are privately owned and operated. Risks associated with this sector's disruption include theft of intellectual property, loss of operations capacity, theft, diversion, and release.[46]

2. **Commercial Facilities Sector:** Commercial Facilities include venues such as shopping malls, hotels and entertainment centers. Risks to this sector include point-of-sale attacks to leverage customer data, intrusions to access trade secrets, correspondence and employee data, and infiltration of systems that could create a negative economic impact.[47]

3. **Communications Sector:** The communications sector enables public information sharing through telephone, internet and broadcasting networks. Cyberattacks to communication networks could be potentially catastrophic, impacting confidential and routine communications as well as the integrity of information communicated in an emergency, and could hamper emergency response.[48]

4. **Critical Manufacturing Sector:** Critical Manufacturing involves the production of essential goods, including machinery, electronics and transportation equipment. Attacks on this sector could leverage industrial control systems to disrupt manufacturing, damage equipment, or steal proprietary information, resulting in supply chain disruptions.[49]

5. **Dams Sector:** The dams sector includes structures used for water storage, flood control and hydroelectric power generation. Cyberattacks on dams could result in the compromise of critical control systems, resulting in flooding, damage to other infrastructure and disruption of water and power supplies.[50]

6. **Defense Industrial Base Sector:** The defense industrial base involves organizations that support military operations, including weapons manufacturing, research facilities and defense contractors. Disruption in this sector can compromise national security, military readiness and defense capabilities.

7. **Emergency Services Sector:** The emergency services sector encompasses those responsible for responding to emergencies, including law enforcement, fire departments, medical services and emergency management. Emergency services have become increasingly reliant on technology for dispatch, communications, data management, security, and access to real-time information to supplement response plans. Cyberattacks on this sector could hamper emergency response resulting in property damage and loss of life.[51]

8. **Energy Sector:** The energy sector includes the generation, transmission and distribution of electricity, oil, natural gas and other energy sources. Many other critical infrastructure sectors rely on this sector to operate, making the energy sector a high-value target for cyberattacks. Disruptions in this sector are potentially catastrophic.[52]

9. **Financial Services Sector:** The financial services sector includes banks, stock and commodity exchanges and insurance companies. It facilitates economic transactions, investments and financial stability. Collectively the organizations that make up this sector are the backbone of the nation's financial system. Disrupting this sector could result in financial crises, loss of personal savings, disruption of business operations and economic instability.[53]

10. **Food and Agriculture Sector:** The food and agriculture sector produces, processes and distributes food and related products. Increasingly this sector is using Industrial Control Systems in processing and production. Because of the relatively recent introduction of internet technology systems within this sector, the risks associated with cyberattacks are not as well understood as other sectors.[54]

11. **Government Facilities Sector:** The government facilities sector comprises assets needed for the functioning of governmental entities, including federal, state and municipal government agencies, school districts, military bases and courthouses. Disrupting this sector could hinder essential government service delivery, harm students and compromise public safety.[55]

12. **Healthcare and Public Health Sector:** The healthcare sector involves medical facilities, pharmaceutical companies and public health agencies. This sector is heavily dependent on internet technologies for the storage and transmission of confidential patient data. Cyberattacks on this sector can result in malicious actors harvesting personal data, corrupting medical records and other information, and impacting the security of the financial systems health care providers rely on. For pharmaceutical companies, these attacks can result in intellectual property theft as well. A large- scale attack on multiple institutions and networked systems has the potential to directly disrupt and negatively impact patient care.[56]

13. **Information Technology Sector:** The information technology sector includes networks, systems, and services that support data storage, processing and communication. Attacks on this sector can lead to cyberattacks, sensitive data breaches and disruption of public communication and essential services, potentially compromising national security.[57]

14. **Nuclear Reactors, Materials and Waste Sector:** This sector involves nuclear power plants, fuel cycle facilities and radioactive waste disposal sites. Cyberattacks on this sector can be particularly dangerous, particularly with regards to the computer-control enabled vehicles that are used in the handling of nuclear materials and waste. In the most extreme scenarios, these attacks could potentially result in faltering power grids, nuclear accidents, release of radioactive materials, environmental contamination and public health risks.[58]

15. **Transportation Systems Sector:** The transportation systems sector includes infrastructure and assets essential for the movement of people and goods, such as airports, seaports, highways and railways. As transportation operations become increasingly reliant on technology, the risks associated with cyberattacks increase. Attacks on this sector also carry

risks to other interdependent sectors. Additionally, the reliance on foreign markets and global supply chains indicates that the financial implications of disruptions to this sector are particularly pronounced.[59]

16. **Water and Wastewater Systems Sector:** The water and wastewater systems sector encompasses facilities that treat and distribute drinking water and the collection and treatment of wastewater. Disruptions to this sector can result in water scarcity, sanitation issues, public health risks and environmental contamination.

Appendix B

Cyberthreat Actors

Cyber threat actors broadly fall into five categories, though at times the lines between these categories are blurred. A cybercrime actor, for instance, may regularly work within organized crime, but that criminal enterprise might also be contracted by a foreign government making them also a state-sponsored actor. Advanced Persistent Threats are frequently state-sponsored actors, but not always. These categories are not mutually exclusive.

State-sponsored actors are directly or indirectly employed by nation states to perpetrate incursions to further the national interests of their employer. Attributing an attack to a state-sponsored actor may be difficult as there is often little evidence to tie the hacker to a nation state. The states responsible for these attacks rarely claim responsibility, and the architecture of the internet allows for a degree of anonymity.[60] These attacks include any attack on the functions of a computer network for a political or national security purpose.[61]

Cybercrime actors are individuals or groups that engage in cybercrime, typically for profit. Some groups may be associated with organized crime, while others operate more autonomously.

Hackers-for-hire is a term for companies that sell their skills as a service to governments, corporations, and individuals. The services they sell include vulnerability and exploit research, malware development, training and support. The European Union Agency for Cybersecurity Threat Landscape 2022 report notes that Interpol has expressed concerns that state-developed cyberweapons will become available on the dark net through hackers-for-hire.[62]

Hacktivists are non-state aligned hackers motivated by ideological factors who utilize hacking as a form of civil disobedience to bring attention to their cause, or to shed light on the actions of their opponents. The term is a portmanteau of “hacker” and “activist”. The most famous among these is Anonymous. Historically hacktivist groups have been few in number and impact.

Advanced Persistent Threats (APTs) are sophisticated and prolonged attacks sometimes carried out by state-sponsored threat actors. APTs aim to steal sensitive data and maintain network access for future exploitation. They often combine multiple attack vectors, such as spear phishing, malware and lateral movement, making it easier to extend and gain access to additional end points within networks.[63]

Appendix C

New York State Reporting Requirements for Cyberattacks and Data Breach Incidents

The timely and accurate reporting of cyberattacks and data breaches is important. Without comprehensive reporting and tracking of incidents, the entities charged with protecting our critical infrastructure cannot respond, investigate, protect or notify affected parties. In New York, there are several mechanisms for oversight and reporting of cyber incidents to sector-specific agencies:

- In 2017, the New York Department of Financial Services (DFS) implemented cybersecurity regulations that were the first of their kind for financial services companies operating in the State. These regulations require companies to maintain robust cybersecurity programs and promptly report incidents to DFS. The program includes regular examinations and assessments of the financial services companies it regulates and provides for penalties in the event of noncompliance.[64]

- In January 2020, the New York State Department of Education (SED) adopted regulations that require certain measures school districts must implement to strengthen student data privacy and security.[65] The regulations require schools, among other things, to adopt a data security and privacy policy, and to report any data breach incident to SED's Chief Privacy Officer within 10 calendar days using a form available on SED's website.[66] In 2022, SED reported receiving 140 data incident reports from schools. Fifty of these incidents were attributed to the actions of third-party contractors and 64 of the incidents were attributed generally to human error (mostly clerical errors).[67] During the audit of SED, for the period March 2020 through April 2021, the audit team reviewed 131 data incidents that had been reported by New York schools.

- The New York State Information Security Breach and Notification Law, as amended by the New York State Shield Act, requires State entities, and any person or business in the State that maintains private information, to report any security breach that may compromise the confidentiality or integrity of private information and requires implementation of reasonable safeguards to protect personal information.[68] Notification of a breach must be given to any New York resident who may be affected. In addition, State entities must notify ITS, the New York State Attorney General's Office (OAG), and the New York Department of State's Division of Consumer Protection (DOS)[69] Companies that experience a breach must notify OAG, DOS and the State Police (in addition to any affected New York residents).The New York State Information Security Policy also requires State government entities to notify the Cyber Command Center of any cyber incident which may have a significant impact on operations or security. [70] While the State Technology Law requires local governments to notify individuals when there is a security breach that compromises private or personal information,[71] there is currently no requirement for local governments to report incidents to a centralized State agency.

Endnotes

[1] See U.S. Securities and Exchange Commission, “SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies,” July 26, 2023, at https://www.sec.gov/news/press-release/2023-139. .

[2] Cybersecurity and Infrastructure Security Agency (CISA), “Critical Infrastructure Security and Resiliency,” at https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (accessed August 29, 2023); and U.S. Department of Homeland Security (DHS) Science and Technology Directorate, “Critical Infrastructure,” at https://www.dhs.gov/science-and-technology/critical-infrastructure (accessed August 29, 2023).

[3] Leila Sharma, “The Download: Feature Articles, Phishing, Spear Phishing, and Whaling,” *New York University* , September 29, 2022, at https://www.nyu.edu/life/information-technology/about-nyu-it/nyu-it-news/the-download/the-download-features/phishing-spear-phishing-whaling.html; and European Union Agency For Cybersecurity (ENISA), “Incident Response: Phishing/Spear Phishing,” at https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing (accessed August 30, 2023).

[4] U.S. Office of the Director of National Intelligence (ODNI), “Counterintelligence Tips: Spear Phishing and Common Cyber Attacks,” at https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf (accessed August 30, 2023).

[5] Federal Bureau of Investigation, Internet Crime Complain Center (IC3), “Common Scams and Crimes: Business Email Compromise,” at https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise (accessed August 30, 2023).

[6] IC3, “Common Scams and Crimes: Ransomware,” at https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (accessed September 21, 2023).

[7] CISA, “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years,” May 7, 2023, at https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[8] CISA Cybersecurity Alert, “Supply Chain Compromise,” January 7, 2021, at https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise.

[9] New York City Department of Education, “Data Security Incidents: Update on MOVEit Data Incident,” at https://www.schools.nyc.gov/about-us/policies/data-privacy-and-security-policies/data-security-incidents (accessed August 30, 2023).

[10] Steve Hughes, “Damage from Albany, N.Y., Cyberattack Dates Back to 2017”, Govtech, March 9, 2021 at https://www.govtech.com/security/damage-from-albany-ny-cyber-attack-dates-back-to-2017.html; and WRGB CBS 6 News, “Ransomeware attack affects 911 dispatch system in three counties”, March 17, 2021, at https://cbs6albany.com/news/local/computer-intrusion-affects-albany-county-911-dispatch-system

[11] IC3, “Internet Crime Report: 2022,” at https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

[12] For more information about the IC3 data, see Appendix B of the “Internet Crime Report: 2022.”

[13] These data include complaints to IC3 (by individuals, businesses, and government entities) that were categorized into these crime types by the IC3. While there are other major crime types that affect critical infrastructure sectors (such as DDoS and Botnet), these five crime types were used for this report because they provided the most consistent and comparable data year-over-year.

[14] IC3, “Internet Crime Report: 2022,” and “Internet Crime Report: 2016,” at https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf. Monetary losses reported in the IC3 data may be artificially low since they do not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim.

[15] IC3, “Internet Crime Report: 2022,” p. 3.

[16] IC3, “Ransomware, What It Is & What To Do About It”, at https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf.

[17] James T Mulder, “Syracuse ransomware attack: School district expects to pay $50,000, insurance pays rest”, Syracuse.com, July 12, 2019 at https://www.syracuse.com/news/2019/07/syracuse-city-schools-computer-systems-under-attack.html.

[18] Sarah Maslin Nir, “How a Cyberattack Plunged a Long Island County Into the 1990s,” *New York Times*, November 28, 2022, at https://www.nytimes.com/2022/11/28/nyregion/suffolk-county-cyber-attack.html.

[19] Sarah Maslin Nir, et al., “Cyberattack Hits Brooklyn Hospitals That Serve Poor New Yorkers,” *New York Times*, December 12, 2022, at https://www.nytimes.com/2022/12/12/nyregion/brooklyn-hospital-cyberattack.html; and Johnson v. One Brooklyn Health, Supreme Court of the State of New York, County of Kings, Index Number 512485/2023, April 26, 2023

[20] New York State Technology Law section 208; General Business Law section 899-aa.

[21] Section 208 (8) of the State Technology Law.

[22] U.S. Securities and Exchange Commission, “Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” at https://www.sec.gov/rules/2022/03/cybersecurity-risk-management-strategy-governance-and-incident-disclosure (accessed August 30, 2023).

[23] See Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 1038 (March 2022); CISA, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet,” at https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf (accessed August 30, 2023).

[24] U.S. Federal Register, Vol. 87, No. 175, September 12,2022/Notices, pp. 55, 830-55.

[25] See CISA, at https://www.cisa.gov/about (accessed August 30, 2023); and “Cyber Threats and Advisories,” at https://www.cisa.gov/topics/cyber-threats-and-advisories (accessed August 30, 2023).

[26] U.S. National Security Agency, at https://www.nsa.gov/Cybersecurity/ (accessed August 30, 2023).

[27] FBI, “National Cyber Investigative Joint Task Force, at https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force (accessed August 30, 2023).

[28] The White House, *National Cybersecurity Strategy*, March 2023, at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; and The White House, *National Cybersecurity Implementation Plan*, July 2023, at https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

[29] DHS, *Cybersecurity Strategy*, May 15, 2018, at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

[30] See New York State Division of Homeland Security and Emergency Services (DHSES), at https://www.dhses.ny.gov/critical-infrastructure-protection-unit (accessed August 31, 2023).

[31] New York State Police Counter Terrorism Unit and NYS Intelligence Center, at https://troopers.ny.gov/counter-terrorism (accessed August 31, 2023).

[32] DHSES, “Critical Infrastructure Protection Unit,” at https://www.dhses.ny.gov/critical-infrastructure-protection-unit (accessed August 31, 2023); DHSES, “Cyber Incident Response Team,” at https://www.dhses.ny.gov/cyber-incident-response-team (accessed August 31, 2023).

[33] Center for Internet Security, Multi-State Information Sharing and Analysis Center, at https://www.cisecurity.org/ms-isac/ (accessed August 30, 2023).

[34] See e.g. CBS News, WRGB Albany, “Ransomware Attack Affects 911 Dispatch System in Three Counties,” March 17, 2021, at https://cbs6albany.com/news/local/computer-intrusion-affects-albany-county-911-dispatch-system; Diego Mendoza-Moyers, “Albany Attacked by Ransomware Hack, Mayor Says,” *The Times Union*, March 30, 2019, at https://www.timesunion.com/news/article/City-of-Albany-attacked-by-ransomware-hack-13728996.php; Sarah Eames, “Chenango County, N.Y., Computers Hit with Ransomware Attack,” *The Daily Star,* October 28, 2020, retrieved at https://www.govtech.com/security/chenango-county-ny-computers-hit-with-ransomware-attack.html; Eric Anderson, “Ransomware Attacks Airport Authority's Servers,” *The Times Union,* January 9, 2020, at https://www.timesunion.com/business/article/Ransomware-attack-cripples-airport-authority-s-14963401.php; Katie Sullivan Borrelli, “Broome County Security Breach Put Employees' and Clients' Personal Information at Risk,” *Press Connects*, May 31, 2019, at https://www.pressconnects.com/story/news/public-safety/2019/05/31/data-security-breach-broome-ny-employee-client-information-risk/1304137001/.

[35] OSC, Division of State Government Accountability (SGA), “Oversight of Water Supply Emergency Plans,” Audit Report 2021-S-39, June 2023, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21s39.pdf.

[36] In 2013, for example, a water dam in Rye, New York was targeted by foreign attackers who were able to infiltrate the dam’s internet connection (see Tracy Connor et al., “Iranian Hackers Claim Cyber Attack on New York Dam,” *NBC News*, December 23, 2015, at https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyberattack-new-york-dam-n484611.

[37] SGA, "Privacy and Security of Student Data," Audit Report 2021-S-29, May 2023, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21s29.pdf; see also Kathleen Moore, "New York Audit: School Districts Unprepared for Cyber Attacks," *The Times Union*, May 16, 2023, at https://www.timesunion.com/education/article/state-audit-school-districts-not-prepared-18102138.php.

[38] See U.S. Government Accountability Office, "Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity," October 20, 2022, https://www.gao.gov/products/gao-23-105480.

[39] SGA, "Letter: Cyber Incident Response Team Report," Audit Report 2020-S-58, November 12, 2021, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2022-20s58.pdf.

[40] SGA, "Letter: Cyber Incident Response Team Report," Follow Up Audit Report 2023-F-8, July 20, 2023, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-23f8.pdf.

[41] SGA, "Controls and Management of the Unemployment Insurance System," Audit Report 2021-S-3, November 2022, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21s3.pdf.

[42] SGA, "Letter: Windows Domain Administration and Management," Audit Report 2022-S-19, May 31, 2023, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-22s19.pdf.

[43] SGA, "Letter: Use of Federal Funding for Election Technology and Security," Audit Report 2020-S-18, September 17, 2021, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2021-20s18.pdf, and Follow up, June 22, 2023, https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-22f35.pdf.

[44] SGA, "User Access Controls Over Selected System Applications," Audit Report 2019-S-34, June 2020, at https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2020-19s34.pdf.

[45] See OSC, Local Government Management Guides, "Information Technology Governance," December 2021, at https://www.osc.state.ny.us/files/local-government/publications/pdf/information-technology-governance.pdf; "Ransomware," October 2019, https://www.osc.state.ny.us/files/local-government/publications/pdf/ransomware.pdf; and "Industrial Control Systems Cybersecurity," October 2019, https://www.osc.state.ny.us/files/local-government/publications/pdf/industrialcontrolsystems.pdf.

[46] CISA, "Introduction to the Chemical Sector Risk Management Agency," at https://www.cisa.gov/sites/default/files/publications/Chemical%2520SRMA%2520Fact%2520Sheet_508.pdf (accessed August 31, 2023).

[47] DHS, "Commercial Facilities Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp.10, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf.

[48] DHS, "Communications Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp.7, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf.

[49] DHS, "Critical Manufacturing Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp. 5, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-critical-manufacturing-2015-508.pdf.

[50] DHS, "Dams Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp.8, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf.

[51] DHS, "Emergency Services Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp.8, at https://www.cisa.gov/sites/default/files/publications/emergency-services-sector-specific-plan-112015-508.pdf.

[52] DHS, "Energy Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp.14, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

[53] DHS, "Financial Services Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp. 8, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf.

[54] DHS, "Food and Agriculture Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp. 6-7, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf.

[55] DHS, "Government Facilities Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp. 9, at https://www.cisa.gov/sites/default/files/2023-03/nipp-ssp-government-facilities-2015-508.pdf.

[56] DHS, "Healthcare and Public Health Sector-Specific Plan," May 2016, pp. 9-10, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf.

[57] DHS, "Information Technology Sector-Specific Plan: An Annex to the NIPP 2013," 2016, pp. 3-5, at https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508 %281%29.pdf.

[58] DHS, "Nuclear Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pp. 10, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf.

[59] DHS, “Transportation Systems Sector-Specific Plan,” 2015, pp. 6, at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf.

[60] Delbert Tran, “Note: The Law of Attribution: Rules for Attributing the Source of a Cyberattack,” *The Yale Journal of Law & Technology,* vol. 20, pp. 376, 381, 2018, at https://yjolt.org/law-attribution-rules-attributing-source-cyberattack.

[61] Oona Hathaway et al., “The Law of Cyberattack,” *California Law Review,* vol. 100, no. 4, pp. 817, 826, August 2012.

[62] European Union Agency for Cybersecurity, “ENISA Threat Landscape 2022”, November 2022, pp.37, at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[63] See e.g. CISA Cybersecurity Advisory, “Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets,” Last Revised December 1, 2020, at https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-296a.

[64] 23 NYCRR Part 500; see also New York State Department of Financial Services, “Proposed Second Amendment to 23 NYCRR Part 500, at https://www.dfs.ny.gov/industry_guidance/cybersecurity; and “DFS HARRIS ANNOUNCES $4.25 MILLION CYBERSECURITY SETTLEMENT WITH ONEMAIN FINANCIAL GROUP LLC,” May 25, 2023, at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202305251.

[65] Education Law 2-d and Part 121 of the Commissioner of Education’s Regulations. For more details on the requirements of Part 121 on school districts, see New York State Department of Education (SED), “Legal Notices and Resources,” at https://www.nysed.gov/data-privacy-security/legal-notices-and-resources.

[66] See SED, “Chief Privacy Officer’s 2022 Annual Report on Data Privacy and Security,” at https://www.nysed.gov/sites/default/files/programs/data-privacy-security/annual-report-on-data-privacy-and-security-2022_0.pdf. A data breach is broadly defined as “the unauthorized acquisition, access, use or disclosure of student, teacher and/or principal data” (Part 121.1[a]).

[67] SED, Chief Privacy Officer’s 2022 Annual Report on Data Privacy and Security.

[68] New York State Technology Law section 208; General Business Law section 899-aa.

[69] See New York State Office of Information Technology Services, “NYS Information Security Breach and Notification Act,” https://its.ny.gov/breach-notification-and-incident-reporting; Office of the New York State Attorney General, “Report a Data Breach,” https://ag.ny.gov/resources/organizations/data-breach-reporting.

[70] See New York State Office of Information Technology Services, “Breach Notification and Incident Reporting,” at https://www.its.ny.gov/incident-reporting.

[71] Section 208 (8) of the State Technology Law.

Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.state.ny.us

Prepared by the Office of Budget and Policy Analysis

Andrea Miller, Executive Deputy Comptroller
Maria Doulis, Deputy Comptroller
Todd Scheuermann, Assistant Deputy Comptroller
Joshua Simons, Policy Director
Sara Kenney, Policy Analyst