APPENDIX

New Jersey Cybersecurity & Communications Integration Cell

Cybersecurity Strategic Plan 2021-2025

IX

NEW JERSEY CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

A Division of the New Jersey Office of Homeland Security & Preparedness

VISION STATEMENT

A safe, secure, and resilient New Jersey that is able to fully realize the opportunities and benefits of technological innovations that act as an engine for economic growth and societal gains.

MISSION STATEMENT

To lead and coordinate New Jersey's cybersecurity efforts while building resiliency to cyber threats throughout the State.

CORE VALUES

SERVICE. We put our State and its citizens first, and we put Mission before self. We take pride in being timely, agile, and relevant.

TEAMWORK. We stand with and behind each other. We recognize that partnerships, both internal and external, are critical to achieving success. We cannot fulfill our Mission alone.

EXCELLENCE. We take great pride in the quality of our work. We do every task, every project, every initiative, to the best of our ability.

DIVERSITY. We strive to build a workforce that is as diverse as New Jersey's citizenry. We pride ourselves on encouraging diversity of thought, perspective, and problem solving.

INTEGRITY. We are committed to holding ourselves accountable to the highest moral and ethical standards in our personal and professional conduct. We can be relied upon to act with honor and truthfulness.

2x

TABLE OF CONTENTS

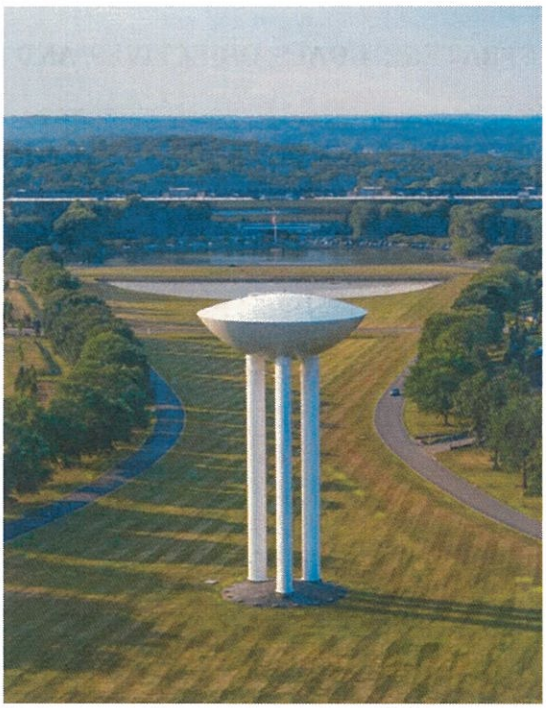
3X

INTRODUCTION

The development of transistor technology at New Jersey's Bell Labs over 70 years ago ushered in the information age that has transformed the global economy, revolutionized public and private sector institutions, created entirely new industries, and transformed all facets of work, life, and play. At the information age's outset, computers were considered systems of record that helped humans process and store information. Over time, increases in computing power, information storage, and communications enabled computers to evolve from systems of record, to systems of engagement, and now, to systems of interaction. Today, computers are embedded into virtually all physical objects that connect, share, and interact with one another, blurring the lines between the physical and cyber worlds. A new car, for example, has upwards of 50 embedded computers that monitor, control, and communicate with everything from its engine to its safety and entertainment systems, as well as surrounding vehicles and other external systems and devices. Beyond automobiles, connected computers are used to enable and control almost all aspects of business and manufacturing, government services, health care, education, communications, lifeline critical infrastructure, and modern conveniences.

The increasing pace of change and rapid technological advances in areas such as elastic cloud computing, artificial intelligence, autonomous systems, big data, and the Internet of Things (IoT) enables modern society to address classes of applications that were inconceivable just a few years ago, while also creating an Internet of Everything (IoE) comprised of physical and virtual objects, people, processes, and data. This digital transformation and our growing dependence on the confluence of technologies is expected to continue unabated for the foreseeable future, creating an expanding attack surface that provides opportunities for nation states, terrorist organizations, political activists, and criminals to maliciously target cyber infrastructure and information for foreign policy/national interests, financial gain, to foment chaos and anarchy, to sow social division, and for other nefarious motivations.

As New Jersey aspires to develop and grow an innovation economy, in which entrepreneurship and innovation are crucial components for long term economic prosperity and societal gains, it must also create a cyber ecosystem that develops a trustworthy environment and helps to manage cybersecurity risks.

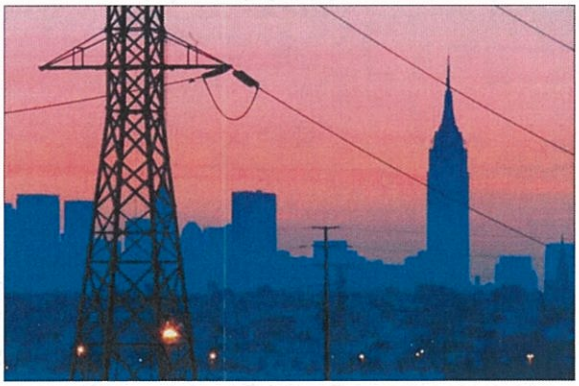


THREAT ENVIRONMENT

Cybersecurity attacks made headlines and garnered the public's attention as a result of large scale and increasingly frequent data breaches beginning with the breach of Target in 2013 that resulted in the compromise of over 40 million Target customers' payment card data. Since that time, numerous public and private sector organizations have fallen victim to data breaches in which financial account information, Social Security numbers, health records, and

4x

other sensitive personally identifiable information of millions of individuals were stolen. And while these attacks are most relatable to the individuals - the general public - whom they impact, even more nefarious cyberattacks have targeted physical systems, threatening lifeline critical infrastructure sectors including electricity, water, transportation, and communications.



Cyberattacks are increasing, both in prevalence and disruptive potential. Since 2019, over 1,500 cybersecurity incidents were reported to the NJCCIC by impacted individuals and organizations. Among the most damaging to NJ institutions in both costs and debilitating operational impacts were the more than 120 reported ransomware attacks, with victims including police departments, municipal and county governments, school systems, health care organizations, utilities, and private businesses. Reporting cybersecurity incidents to the NJCCIC is voluntary for most organizations. As such, it is estimated that the true number of incidents is much greater than the numbers reported.

Cyberattacks are not constrained by geographic boundaries; attacks launched against systems in geographies outside New Jersey may have collateral effects that threaten and/or impact individuals and institutions in the State. Conversely, cyberattacks launched against networks and systems in New Jersey may have cascading effects across the region, the nation, and the world. The capability to carry out crippling attacks is not solely the domain of nation state actors. Individual criminals and criminal syndicates, hacktivists, terrorist groups, and other threat actors can carry out destructive and costly attacks for a host of motivations. Such attacks ultimately lead to the loss of critical information and information systems that threaten public safety, undermine public confidence, have a negative effect on the economy and diminish the security posture of the State of New Jersey and, more broadly, the United States.

Whether you're an individual or a public or private sector organization, you are not immune to cyberattacks. On a monthly basis, the NJCCIC detects and blocks over 10 million attacks targeting New Jersey State Government networks, systems, and users. Anything and anyone connected to the Internet can be a target. As with physical defenses, it is unrealistic to think that even the most steadfast cyber defenses are impenetrable. Recognizing this, the NJCCIC strategic plan not only incorporates cyber prevention goals and objectives intended to mitigate the risks and impacts of cyberattacks, but also includes equal focus on building capabilities necessary to detect, respond to, and recover from them, thereby making New Jersey more resilient to the inevitability of successful cyberattacks.

> *"It's clear where the world is going. We're entering a world where every thermostat, every electrical heater, every air conditioner, every power plant, every medical device, every hospital, every traffic light, every automobile will be connected to the Internet. Think about what it will mean for the world when those devices are the subject of attack." Then he made his pitch. "The world needs a new, digital Geneva Convention."*
>
> — Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

5x

THE THREAT ENVIRONMENT
TIMELINE OF NOTABLE GLOBAL CYBERSECURITY INCIDENTS

- In 2013, Iranian hackers associated with the Islamic Revolutionary Guard infiltrated the controls of a small dam located approximately 20 miles north of New York City.
- In December of 2015, Russian state-sponsored hackers launched cyberattacks against the Ukraine power grid causing the first cyber-induced blackouts that affected hundreds of thousands of homes and businesses.
- In June of 2016, Russian hackers infiltrated the online voter registration systems of the states of Illinois and Arizona, and carried out other cyber and influence operations in attempts to impact the integrity of the election processes in the United States.
- Also in 2016, the largest ever distributed denial-of-service attack involving thousands of Internet of Things devices was launched against Domain Services Provider Dyn DNS, resulting in an outage that affected approximately 1/3 of the internet. Notably, the malicious code that was used to carry out this attack was created by a NJ resident, Paras Jha, who was subsequently arrested and prosecuted.
- In 2017, two of the most destructive cyberattacks affected systems worldwide. The May 2017 Wannacry ransomware attack that has since been attributed to North Korean state sponsored hackers impacted approximately 300,000 computers across 150 countries, including in the UK where hospitals and clinics were forced to turn away patients and cancel operations.
- Then in June, NotPetya, the most destructive cyberattack in history impacted thousands of organizations worldwide causing over $10 billion in losses and damages. New Jersey-based Merck Pharmaceuticals was one of the victim organizations, which not only cost Merck hundreds of millions in financial damages but also impacted its ability to produce critical vaccines. Another NotPetya victim, Maersk, saw its ability to conduct shipping operations crippled and caused the shutdown of the Port of Newark. Losses and damages related to NotPetya for just Merck and Maersk are estimated at $1.2 billion. NotPetya has since been attributed to Russian state-sponsored hackers.
- In March of 2018, the US Department of Justice indicted nine Iranian hackers alleged to have carried out attacks against more than 300 universities in the United States and abroad.
- In November 2018, Starwood Hotels confirmed its hotel guest database of about 500 million customers had been stolen in a data breach. The hotel and resorts giant said in a statement filed with US regulators that the "unauthorized access" to its guest database was detected on or before September 10, 2018 — but may date back as far as 2014.
- In 2019, a cloud database configuration vulnerability was exploited, resulting in the breach of over 100 million Capital One customers.
- In 2020, cyber criminals and nation states have acted to exploit the COVID-19 pandemic through various cyber scams and frauds for financial gain, and intrusions targeting intellectual property related to response strategies, and potential vaccines and treatments research.

6X

NEW JERSEY'S APPROACH TO CYBERSECURITY

The mission of the New Jersey Office of Homeland Security and Preparedness is to lead and coordinate New Jersey's counterterrorism, cybersecurity, and preparedness efforts.

Executive Order No. 5 signed by Governor Corzine on March 16, 2006, established the New Jersey Office of Homeland Security and Preparedness (NJOHSP) as the State Agency responsible for administering, coordinating, leading, and supervising New Jersey's counter terrorism, and preparedness efforts. NJOHSP is led by a Director, who also acts as the State's Homeland Security Advisor and the Chair of the Domestic Security Preparedness Task Force, which in accordance with the New Jersey Domestic Security Preparedness Act P.L. 2001 c.246, is responsible for effectuating the coordination of the disaster preparedness and recovery resources, as well as the management, coordination, administration of responses to any terrorist attack or any other technological disaster.

As a result of Executive Order No. 178, signed by Governor Christie on May 20, 2015, the NJOHSP, through a newly formed component organization, the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), was tasked with leading and coordinating New Jersey's cybersecurity efforts while building resiliency to cyber threats throughout the State. By organizing cybersecurity under the NJOHSP, the State centralized responsibility and accountability for statewide cybersecurity efforts, beyond just those of New Jersey State Government networks, systems, and information. Located at New Jersey's Regional Operations and Intelligence Center (ROIC) and, acting in a combined cyber fusion and security operations center capacity, the NJCCIC is staffed by personnel from the NJOHSP, the New Jersey Office of Information Technology (NJOIT), and the New Jersey State Police (NJSP), thereby providing a multi-agency and multi-disciplinary "all threats/all hazards" approach to cybersecurity.

In addition to the three primary agencies that comprise the NJCCIC, partnerships with a number of other key stakeholders have been developed, including but not limited to, the New Jersey Office of the Attorney General, the New Jersey National Guard, the New Jersey Board of Public Utilities, the Federal Bureau of Investigation, the US Department of Homeland Security; national information security organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), Health Information Sharing and Analysis (H-ISAC), Financial Services Information Sharing and Analysis Center (FS-ISAC), and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC); as well as public and private sector organizations and operators of critical infrastructure and key resources throughout New Jersey and beyond. These partnerships ensure critical information is shared broadly and key resources are coordinated across applicable sectors in a whole-of-state approach to cybersecurity in New Jersey. At the same time, the NJCCIC realizes that, while its focus is on making New Jersey more resilient to cyberattacks, it also has a role to play in making the region, the nation, and the world more resilient.

"Cyber security is an information technology issue, but not only an information technology issue. It is a law enforcement issue, but not only a law enforcement issue. It is a national and homeland security issue, but not only those things. New Jersey, by combining the three in its approach to dealing with cyber security seems to be offering up an important model – "the Garden State model" - of how the sad state of cyber security can begin to get better, and how states can contribute to that improvement."

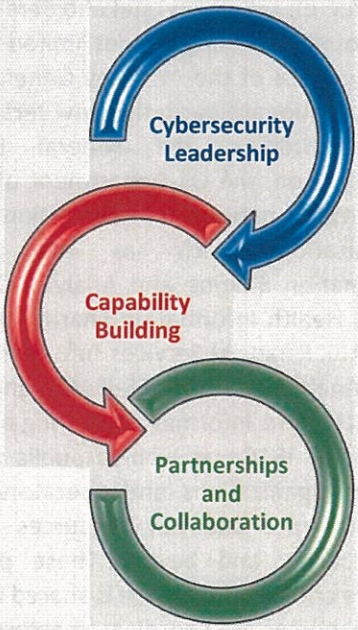
- The Center for Information Security at Stanford Law School

7x

STRATEGIC PLAN GOALS, OBJECTIVES, AND ACTION ITEMS

This strategic plan represents a pathway to achieving improved cyber resilience through the prosecution of a series of interrelated goals, objectives, and action items intended to help safeguard New Jersey's institutions, businesses, and individuals. It includes broad statewide goals and objectives applicable to all public and private sector institutions and individuals, as well as those specific to the executive branch of New Jersey State Government, for which the NJCCIC has direct oversight. This strategic plan also supports the overall mission of the New Jersey Office of Homeland Security and Preparedness, whereby cybersecurity is woven into its counterterrorism, counterintelligence, and preparedness functions.

NJCCIC STRATEGIC GOALS



Cybersecurity Leadership: Lead and coordinate a whole-of-state approach to cybersecurity.

Capability Building: Increase the resilience of public and private institutions, critical infrastructure assets and key resources, and the citizens of New Jersey.

Partnerships and Collaboration: Cultivate strategic partnerships and pervasively collaborate with public and private sector organizations.

STRATEGIC GOAL 1: CYBERSECURITY LEADERSHIP

Lead and coordinate a whole-of-state approach to cybersecurity.

In 2015, the NJCCIC was established as a component organization within the NJ Office of Homeland Security and Preparedness and was tasked with the responsibility of serving as the central civilian resource for cybersecurity leadership and coordination for a broad range of statewide cybersecurity initiatives and efforts. Since its inception, the NJCCIC has delivered significant public benefit and value in protecting New Jersey's institutions, businesses, and individuals against a growing number of cyber threats. Strategic Goal 1 builds upon those successes and addresses the NJCCIC's role in leading and coordinating a whole-of-state approach to cybersecurity.

OBJECTIVE 1.1: Establish and grow the NJCCIC as a Cybersecurity Center of Excellence (CCOE) that provides leadership, best practices, training, support, and research.

Action Items:

- Provide thought leadership and champion the adoption of cybersecurity best practices and initiatives across New Jersey in the face of new and emerging cybersecurity risks and threats.
- Establish an NJCCIC Cybersecurity Advisory Committee consisting of cybersecurity leaders and subject matter experts from industry, government and non-government organizations, and academia to help provide direction and support for whole-of-state cybersecurity efforts.
- Research, develop, support, and implement innovative processes, practices, and technologies in order to improve the efficiency and effectiveness of New Jersey's cybersecurity efforts.
- Update and align New Jersey's cybersecurity strategy to meet evolving threats and societal needs.
- Take an active role in leading and influencing national cybersecurity initiatives.
- Develop strategies and tactics necessary to address threats introduced by the continued digital transformation of work and society (e.g. IoT, 5G, smart cities, artificial Intelligence, autonomous vehicles, etc.).
- Support and participate, where appropriate, in private sector and academic cybersecurity research and development initiatives.
- Identify and attain grant funding to support the development and implementation of innovative cybersecurity programs of work, practices, and technologies.

OBJECTIVE 1.2: Champion and grow a culture of cybersecurity and privacy across executive branch departments and agencies.

Action Items:

- Develop, adopt, and institute cybersecurity best practices, standards, and frameworks across executive branch departments and agencies.
- Institute a continuous improvement program that measures, assesses, and implements policies, processes, standards, and technologies necessary to establish sufficient assurance levels are maintained for systems and program maturity.
- Ensure cybersecurity investments are risk-based and provide prioritized protections for New Jersey's most critical and sensitive assets.

OBJECTIVE 1.3: Promote and implement cybersecurity education and training initiatives.

Action Items:

- Continue collaboration with NJ Department of Education on the development of a statewide computer science curriculum that integrates cybersecurity education.
- Partner with K-12 and higher education institutions to develop cybersecurity education and training programs.
- Continue to coordinate and grow participation in hands-on educational opportunities for K-12 and higher education students, including programs, such as Girls Go CyberStart program, Cyber Patriot, Capture the Flag, etc.
- Grow and support cybersecurity internship, apprenticeship, and scholarship for service programs necessary to develop a capable cyber workforce.
- Support and implement cybersecurity training and education initiatives for professional development and reskilling current workers.

OBJECTIVE 1.4: Advocate for and support legislative efforts and government initiatives that improve cybersecurity posture of the State.

Action Items:

- Provide reports to legislative committees on cybersecurity threats, risk posture, and best practices.
- Monitor, review, and provide input on legislation that includes a cybersecurity nexus.
- Support legislative and regulatory activity that promotes cybersecurity and data privacy protections.
- Provide input and support for efforts to consolidate accountability for harmonizing the cybersecurity policies, budgets, and responsibilities necessary to achieve uniformity and the overall improvement of the cybersecurity postures of executive branch departments and agencies.
- Support efforts to create cybersecurity jobs and expand the cybersecurity industry in New Jersey.
- Lead and support efforts to improve inefficient state government business processes and unnecessary bureaucratic structures that introduce unnecessary risk and act as obstacles to achieving cyber resilience.

10X

OBJECTIVE 1.5: Measure, assess, and drive improvements to the New Jersey's cybersecurity posture.

Action Items:

- Expand implementation of intelligence-driven cybersecurity efforts.
- Prioritize cybersecurity investments based on risk.
- Collect, process, and analyze security telemetry and threat data to aid in identifying emerging threats, trends, and risk management strategies.
- Develop dashboards and produce cybersecurity progress reports to key stakeholders that identify trends, risks, emerging threats, and key performance indicators.

STRATEGIC GOAL 2: CAPABILITY BUILDING

Increase the security posture and resilience of public and private institutions, critical infrastructure assets and key resources, and the citizens of New Jersey by building cybersecurity capabilities.

Resilience, as defined by Presidential Policy Directive PPD-21, is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Cyber resilience focuses on the preventive, detective, and reactive controls in an information technology environment to assess gaps and drive enhancements to improve the overall security posture of the entity. This strategic goal addresses the State's cybersecurity readiness and cyber resilience, including those initiatives and activities necessary to prepare for, respond to, and recover from cyberattacks.

OBJECTIVE 2.1: Develop and implement a cybersecurity risk management program.

Action Items:

- Build the necessary structures and processes to assess and manage cyber risk across New Jersey.
- Update, as appropriate, the Statewide Information Security Manual that prescribes a risk–based approach to information security while establishing the required behaviors and controls necessary to protect information technology resources, secure personal information, safeguard privacy, and maintain the physical safety of individuals.
- Develop and grow the capability to conduct cybersecurity surveys and assessments of public and private sector cybersecurity programs and systems.
- Develop and implement a supply chain security program that establishes baseline requirements and institutes a vendor assessment platform through which security due diligence assessments are standardized and shared with relevant stakeholders.

11X

- Develop a security assessment function that ensures the security and privacy controls for major systems and applications, and general support systems in the executive branch of New Jersey State Government are assessed, and risks are managed to acceptable levels, prior to deployment to operational status.

- Continually test executive branch networks, systems, and applications to identify vulnerabilities, gaps in cyber defenses, and emerging threats.

- Engage independent third parties to review and assess the appropriateness of the cybersecurity program and the controls that safeguard executive branch systems.

OBJECTIVE 2.2: Fortify New Jersey's cyber defenses.

Action Items:

- Provide direct and indirect support to executive branch and other public and private sector organizations in implementing cybersecurity best practices and technologies.

- Expand the breadth, capability, and effectiveness of the NJCCIC's managed security services.

- Research, identify, acquire, deploy, and monitor effective preventive and detective security technologies and services.

- Establish uniformity of cybersecurity controls, technologies, and processes across executive branch departments and agencies.

- Partner with the NJ Office of Information Technology and other executive branch departments and agencies to develop a technology roadmap that incorporates security and privacy by design.

- Lead and support efforts to modernize and harden New Jersey's technology infrastructure.

- Increase the security posture (people, process, technology) for a remote workforce environment.

- Leverage data analytics to identify threats and implement controls to safeguard against them.

OBJECTIVE 2.3: Increase the capacity to respond to and recover from significant cyber incidents.

Action Items:

- Continue to develop the NJCCIC Security Operation Center's monitoring, alerting, and response capabilities to identify and effectively respond to cybersecurity incidents.

- Develop and publish an incident response plan to include a defined methodology and individual playbooks necessary to ensure a consistent and organized response to incidents.

- Develop and implement tools, technologies, and practices for use in handling cybersecurity incidents.

- Develop, conduct, and participate in cybersecurity incident response exercises internally with executive branch departments, and externally with public and private sector organizations.

- Enhance coordination of cybersecurity incident handling among federal, state, and local partners, including emergency management teams and operators of critical infrastructure and key resources.

- Develop NJCCIC capabilities that augment an impacted organization's capabilities to respond to and recover from a cybersecurity incident.

- Establish a New Jersey Cyber Corps comprised of public and private sector resources that can provide assistance in response to and recovery from significant cybersecurity incidents.

- Periodically review the Cybersecurity Annex to the State Emergency Operations Plan for appropriateness and relevance, and update as necessary.

OBJECTIVE 2.4: Establish a cyber talent management program that attracts, develops, and retains highly skilled and capable cybersecurity professionals.

Action Items:

- In partnership with the Civil Service Commission, develop cybersecurity titles and career tracks to meet current and future needs of state and local governments in attracting and retaining capable cybersecurity professionals.

- Provide executive branch cybersecurity personnel with resources and opportunities to continually improve and develop knowledge, skills, and abilities required to address evolving cybersecurity challenges and to enable career advancement opportunities.

- Further develop and expand the NJCCIC's internship, apprenticeship, and scholarship opportunities.

OBJECTIVE 2.5: Lead and support efforts that increase the capability and capacity of all New Jerseyans to recognize and mitigate cyber risks.

Action Items:

- Develop, implement, and deliver online and in-person cybersecurity training offerings for public and private sector organizations, individual citizens, and community organizations.

- Develop and distribute relevant security awareness materials, alerts, and advisories, and provide notifications to key stakeholders of new and/or updated statutes, regulatory requirements, and policies.

- Implement a virtual cyber range to provide hands-on cybersecurity and incident handling training to government and non-government entities and individuals.

- Conduct regular cybersecurity exercises to test and improve the ability of executive branch employees to identify and mitigate risks.

OBJECTIVE 2.6: Protect New Jersey elections from cyber threats and influence operations.

Action Items:

- In partnership with the NJ Secretary of State's Office, provide cybersecurity support in securing state and local elections systems.

- Develop a taskforce and coordinate elections security efforts across state, federal, local, and non-government partner organizations.

- Champion and drive cybersecurity best practices, standards, frameworks, and technologies across the elections ecosystem in New Jersey.

- Establish continuous monitoring, alerting, and incident response capabilities specific to elections infrastructure.

- Engage industry partners to help implement solutions that bolster the security of New Jersey's elections infrastructure.

STRATEGIC GOAL 3: PARTNERSHIPS AND COLLABORATION

Cultivate strategic partnerships and pervasively collaborate with public and private sector organizations to increase the capacity and capability to recognize threats, defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and the critical infrastructure of New Jersey and the United States.

Strategic Goal 3 recognizes that, in a hyper-connected world, all organizations face a common set of threats for which a collaborative, whole-of-state approach allows for the sharing of critical information and key resources, and the integration of public and private sector cyber defense and response capabilities. The principle of *One Team/One Fight* whereby many different organizations and individuals come together for a common mission is a key component of this strategic goal.

"One example I'd look at is the New Jersey Cybersecurity & Communications Integration Center, the NJCCIC. And what they've done is outreach to critical infrastructure partners in the state that include private sector partners."

-Timothy Blute, Program Director, NGA Center for Best Practices, Homeland Security & Public Safety Division

OBJECTIVE 3.1: Develop new and strengthen current partnerships.

Action Items:

- Establish strong and improved engagement programs and trusted partnerships with public and private sector organizations, Information Sharing Analysis Centers and Organizations (ISACs and ISAOs), and other non-government cybersecurity organizations.

- Strengthen and grow the partnerships with federal, state, local and NJ National Guard partners to increase the capacity and capability to defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and the critical infrastructure of New Jersey and the United States.

- Integrate and improve public and private-sector cyber defense and response efforts.

- Increase federal and state grant funding utilization to help bolster the cybersecurity posture of critical infrastructure and key resources across New Jersey.

- Improve incorporation of the NJCCIC's programs of work with those of the NJOHSP's counterterrorism, counterintelligence, and preparedness functions.

- Bolster the NJCCIC's role and effectiveness within the NJ Regional Operations and Intelligence Center and expand its engagement with fusion centers throughout the United States.

- Improve coordination of the NJCCIC's statewide cybersecurity efforts with New Jersey Urban Area Security Initiative (UASI) Program representatives to ensure high-threat, high-density urban areas have the appropriate resources to prevent, protect against, mitigate, respond to, and recover from cyberattacks.

- Establish new and grow current partnerships with academia, including K-12, higher education, and private sector educational organizations, to ensure development of required cybersecurity knowledge, skills, and abilities.

OBJECTIVE 3.2: Strengthen the NJCCIC's ability and effectiveness in collecting, analyzing, and disseminating cyber or other relevant information in order to enable potential targets to recognize threats and defend and respond more effectively, reducing the likelihood that those attacks and attackers will succeed.

Action Items:

- Observe, gather, and analyze critical cyber and related information in order to better understand security problems and inter-dependencies related to cyber systems, so as to ensure their confidentiality, integrity, and availability.

- Disseminate relevant and timely cyber and related information to NJCCIC members; federal, state and local governments; and other entities that may be of assistance in preventing, detecting, mitigating, or recovering from the effects of a cyberattack.

- Continue to add relevant cybersecurity content and features to NJCCIC web and social media properties.

- Develop an interactive web portal for cybersecurity communications and information sharing with NJCCIC members.

- Deploy a bi-directional threat intelligence platform for use by public and private sector organizations.

- Author, collaborate on, and publish research papers and articles in trade journals and other relevant publications.

- Expand delivery platforms to include live and recorded audio and video content.

OBJECTIVE 3.3: Communicate and share critical cyber and other relevant information by hosting, coordinating, and participating in cybersecurity symposiums, conferences, workshops, briefings, and events.

Action Items:

- Coordinate and host an annual Statewide Cybersecurity Conference.

- Develop and conduct sector- and audience-specific cyber symposiums, threat briefings, presentations, and workshops.

- Participate as cybersecurity subject matter experts for industry and government conferences and events.

- Develop, host, and participate in online webinars, presentations, and trainings.

CRITICAL SUCCESS FACTORS

The successful execution of this strategic plan will broadly depend on or be influenced by the following considerations.

Management Endorsement - It is essential that this strategic plan is endorsed and driven at the highest levels of the executive branch of New Jersey State Government and that it receives the full support of the Director and Deputy Director of the New Jersey Office of Homeland Security and Preparedness, and the Domestic Security Preparedness Task Force. The Director of the Office of Homeland Security and Preparedness should identify and establish State cybersecurity priorities and provide budgetary and human resources needed to implement the strategy.

Resource Prioritization - As the threat landscape is both evolving and expanding, it is critical to continuously advance New Jersey's security, resilience and operational capacities. The prioritization and fluid allocation of key resources is necessary to maintain currency and effectively protect against and respond to significant cybersecurity incidents.

Shared Responsibility - Cybersecurity is a shared responsibility beyond New Jersey State Government alone. As cyberspace consists of a hyper-connected array of networks, systems, and devices, the cooperation of all key stakeholders – government, industry, non-government organizations, and academia – is essential to not only the success of this strategic plan, but also the public health, welfare, and safety of the citizens, economy, and public interests of the State of New Jersey and national security.

Human Capital - As cybersecurity is a highly technical and complex discipline that requires qualified and skilled human resources at sufficient staffing levels, the ability of the NJCCIC to recruit, develop, and retain talented and mission-focused personnel is critical to carrying out this strategic plan.

Funding - This strategic plan was drafted assuming that funding levels for cybersecurity would remain stable and additional investments would be made over time to address the growing threat environment and to protect the public and private institutions, critical infrastructure assets, and the citizens of New Jersey from the threat of cyberattacks.

AUTHORITIES

New Jersey Domestic Security Preparedness Act P.L. 2001, c.246 establishes a New Jersey Domestic Security Preparedness Task Force that includes the New Jersey Office of Homeland Security and Preparedness, the New Jersey National Guard, the Office of Emergency Management in the Division of State Police, among other state, county, and local organizations in order to maximize, enhance, and effectuate coordination of the disaster preparedness and recovery resources. Included in the duties of the task force is the development, implementation, and management of comprehensive responses to any terrorist attack or any other technological disaster and the effective administration, management, and coordination of remediation and recovery actions and responses following any such attack or disaster.

State of New Jersey Executive Order No. 5 signed by Governor Corzine on March 16, 2006 establishes the New Jersey Office of Homeland Security and Preparedness as the State Agency responsible for administering, coordinating, leading, and supervising New Jersey's counterterrorism and preparedness efforts. NJOHSP is led by a Director, who also acts as the State's Homeland Security Advisor and the Chair of the Domestic Security Preparedness Task Force. The Director and the NJOHSP shall be authorized to call upon the expertise and assistance of all State departments, divisions, and agencies to carry out their mission. The NJOHSP may, to the extent not inconsistent with any other law, employ, consult, and contract with private and public entities, and enter into such agreements with public and private individuals or entities as necessary to further the mission of the Office or of other offices and units that fall under the Director's supervision.

State of New Jersey Executive Order No. 178 signed by Governor Christie on May 20, 2015 establishes the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) as a component organization within the Office of Homeland Security and Preparedness that acts as the central State civilian interface authorized to coordinate cybersecurity information sharing and analysis across all levels of government, agencies, authorities, and the private sector pursuant to 6 U.S.C. § 133 et seq. The NJCCIC is authorized to draw upon the assistance of any department, office, division, or agency of this State to supply it with expertise and assistance, including information and personnel, to carry out the NJCCIC mission. The NJCCIC is composed of representatives of State entities, including the Office of Homeland Security and Preparedness, the Division of State Police, and the Office of Information Technology.

State of New Jersey Technology Circular 17-00-NJOIT, October 14, 2017, establishes a management structure for information security across the executive branch of New Jersey State Government including the roles and responsibilities of the Director of the Office of Homeland Security and Preparedness, the State Chief Technology Officer, the State Chief Information Security Officer, and the Director of the New Jersey Cybersecurity & Communications Integration Cell.

RUSSIA/UKRAINE CYBER THREAT ASSESSMENT AND RISK MITIGATION STEPS

TLP: WHITE | At this time, the NJCCIC is not aware of any specific or imminent cyber threat to NJ. This NJCCIC Advisory is being provided to assist agencies and organizations in guarding against the persistent malicious actions of cybercriminals. As the crisis in Ukraine continues to escalate, it is likely that Russia's aggressive cyber activity will increase and spread beyond their initial Ukrainian government, military, energy, and financial targets. Russia, and those aligned with its efforts, will continue to conduct disruptive and destructive cyberattacks, cyber espionage, and information operations against Ukraine and any governments or groups supporting Ukraine or opposed to Russia's invasion of Ukraine.

INFORMATION OPERATIONS

In the buildup to the invasion of Ukraine, Russia launched misinformation, disinformation, and malinformation (MDM) campaigns in an attempt to establish numerous pretexts for its invasion. Recently, the Russian Security Council voted to recognize the Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Eastern Ukraine as independent while citing the need to protect the people in those regions from purported Ukrainian genocide. Other pretexts include:

- Requests from the DNR and LNR to protect them from Ukrainian aggression
- Russia's need to demilitarize Ukraine
- Ukraine and other former USSR states being part of the "Fatherland"
- Russian security needs
- Alleged Ukraine-sanctioned Nazis
- Alleged corruption and mishandling of Ukrainian affairs
- Western degeneration of social values, US influence

These pretexts are often supported by staged videos and doctored photos claiming to document Ukrainian aggression against Russian troops. Such MDM campaigns are expected to continue using various media platforms to further support Russia's narrative.

CYBER ESPIONAGE

Continued on next page.

19x

Russian intelligence services have a long history of targeting government, military, diplomatic, and other organizations and businesses worldwide for intelligence that benefits Russia's foreign policy and military decision making. Cyber espionage activity will continue to provide Russia with intelligence in support of its activities against Ukraine, as well as its situational awareness of the activities of other nations in response to it. This intelligence will also feed its information operations and be used for further disruptive and destructive cyberattacks.

DISRUPTIVE AND DESTRUCTIVE CYBERATTACKS

As part of its invasion, Russia has launched supporting cyberattacks against military, government, financial, and energy targets in Ukraine. Leading up to the invasion, Russia instigated cyberattacks against various Ukrainian banks, military infrastructure, and government services to sow fear in Ukrainian citizens and undermine their confidence that the State can protect them. This activity follows a long history of Russian-attributed cyberattacks against Ukraine, dating back to at least 2013 when Russia launched attacks against Ukrainian government networks in response to pro-democracy protests throughout Ukraine. In 2014, during Russia's annexation of Crimea, cyberattacks crippled Ukrainian military defenses, including its radar systems. In December of 2015, Russian military intelligence operatives, referred to as Sandworm, launched cyberattacks against the Ukrainian power grid, resulting in power outages for hundreds of thousands in the Kyiv region. The malware used to disable the power grid also wiped and destroyed files on infected computer systems. In 2016, Russian military intelligence refined their malware and automated their cyberattacks against Ukraine's power grid causing more power outages. And in 2017, Russian intelligence services inserted malware into an accounting software update that resulted in the most damaging cyberattack in history. While the malware was intended to target businesses operating in Ukraine, it spread worldwide, including here in NJ where Merck and the Port of Newark were crippled due to the destructive nature of the malware. This cyberattack is known as NotPetya and resulted in over $10B of damages worldwide. As with the power grid attack, the malware used in NotPetya also wiped the computer systems it infected.

More recently, Russian state affiliated actors have launched numerous disruptive and destructive ransomware attacks against targets throughout the world but primarily targeting US institutions. In May of 2021, the Russian-affiliated ransomware group Darkside compromised Colonial Pipeline, crippling the gas supply chain in the Southeastern portion of the United States. Also in May 2021, another Russian-affiliated ransomware group Conti targeted JBS Meats, resulting in

Continued on next page.

20x

supply chain disruptions in the food industry. In NJ, numerous schools, local governments, police departments, and hospitals have been impacted by ransomware attacks over the past several years resulting in significant operational disruptions and financial losses.

RISK MITIGATION STEPS

As more punitive sanctions are levied against Russia in response to its invasion of Ukraine, it is increasingly likely that these disruptive and destructive cyberattacks will spread beyond Russia's Ukrainian targets. All organizations are advised to ensure all preventive, detective, and responsive cybersecurity controls and plans are fully implemented and updated. In particular, organizations should confirm with their respective IT and information security teams that:

- Multi-Factor Authentication (MFA) is implemented for all remote access to internal systems and cloud services that provide critical services or host sensitive information.
- The Principle of Least Privilege is applied such that permissions for a given user account or process is restricted to only those privileges which are essential to perform their intended function.
- Critical vulnerabilities are patched, with priority given to public-facing systems and applications.
- Public-facing web applications are protected by a web application firewall.
- Internal networks are appropriately segmented to contain an attack or malware to a subset of systems and to prevent its widespread propagation.
- Endpoint Detection and Response (EDR) software is installed on all supported endpoints and cloud workloads.
- Current backups are stored offline and have been tested to confirm their viability in fully restoring systems and data.
- All end-of-life systems and applications are decommissioned and powered off.
- Incident response plans within the organization have been updated and a crisis communications contact list includes current emergency contact information for all appropriate personnel.
- Disaster Recovery and Continuity of Operations Plans are current and can be implemented in the event of a loss of services

The NJCCIC is constantly collaborating with federal, state, and local authorities, owners, and operators of critical infrastructure, and other third parties in the private sector to make NJ more

Continued on next page

21x

resilient to cyberattacks. We continuously assess and adjust our cyber capabilities to account for emerging threats. We ask all public and private sector organizations to be diligent in their cyber risk management efforts and to report any suspicious cyber activity to the NJCCIC at cyber.nj.gov or 1-833-4-NJCCIC.

REPORTING

The NJCCIC encourages recipients who discover signs of malicious cyber activity to contact us via the cyber incident report form at cyber.nj.gov/report.

Additional resources can be found on the NJCCIC's website by visiting cyber.nj.gov, as well as cisa.gov/shieldsup

22x

ACTIVE SPEARPHISHING CAMPAIGN TARGETING NJ PUBLIC EMPLOYEES

TLP: WHITE | This NJCCIC Alert is being provided to assist New Jersey public sector members guard against the persistent malicious actions of cybercriminals.

DETAILS

The NJCCIC has been alerted to a spearphishing campaign targeting New Jersey public employees with myNewJersey portal accounts. The spearphishing email uses display name spoofing to appear as though it is sent from "NJ Division of Pensions and Benefits," though the corresponding sender email address is donotreply@cclifestyle[.]net , and uses a subject line of "NJ Division of Pensions and Benefits Reports." The email states that the user has a new document from the NJ Division of Pensions and Benefits and includes a PDF attachment.

From: NJ Division of Pensions and Benefits <donotreply@cclifestyle.net>
Sent on: Friday, February 4, 2022 1:29:30 AM
To: [redacted]
Subject: NJ Division of Pensions and Benefits Reports
Urgent: High

Attachments: NJDPB _4452.pdf (25.33 KB)

WARNING: This email originated from outside your organization. Please use extreme caution before opening any links or attachments.

NJ Division of Pensions and Benefits

Dear : [redacted]

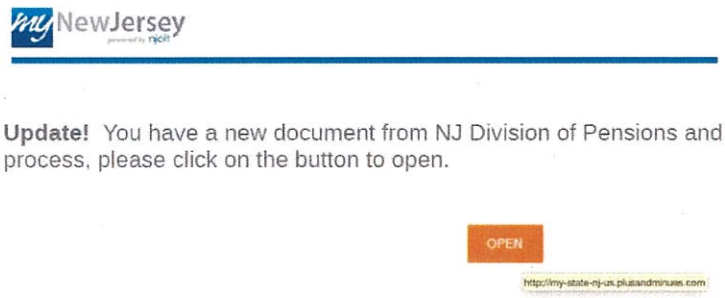
You have a new document from NJ Division of Pensions and Benefits : Thursday, February 3, 2022 _ 8:29:22 PM

Notice: This e-mail message and any attachments to this e-mail message contain information that may be legally privileged and confidential from the State of New Jersey, Department of the Treasury, Pensions & Benefits. If you are not the intended recipient, you must not review, transmit, convert to hard copy, copy, use or disseminate this e-mail or any attachments to it. If you have received this e-mail in error, please immediately notify us by return e-mail and delete this message. If this e-mail contains a forwarded message or is a reply to a prior message, some or all of its contents or attachments may not have been produced by the State of New Jersey, Department of the Treasury.

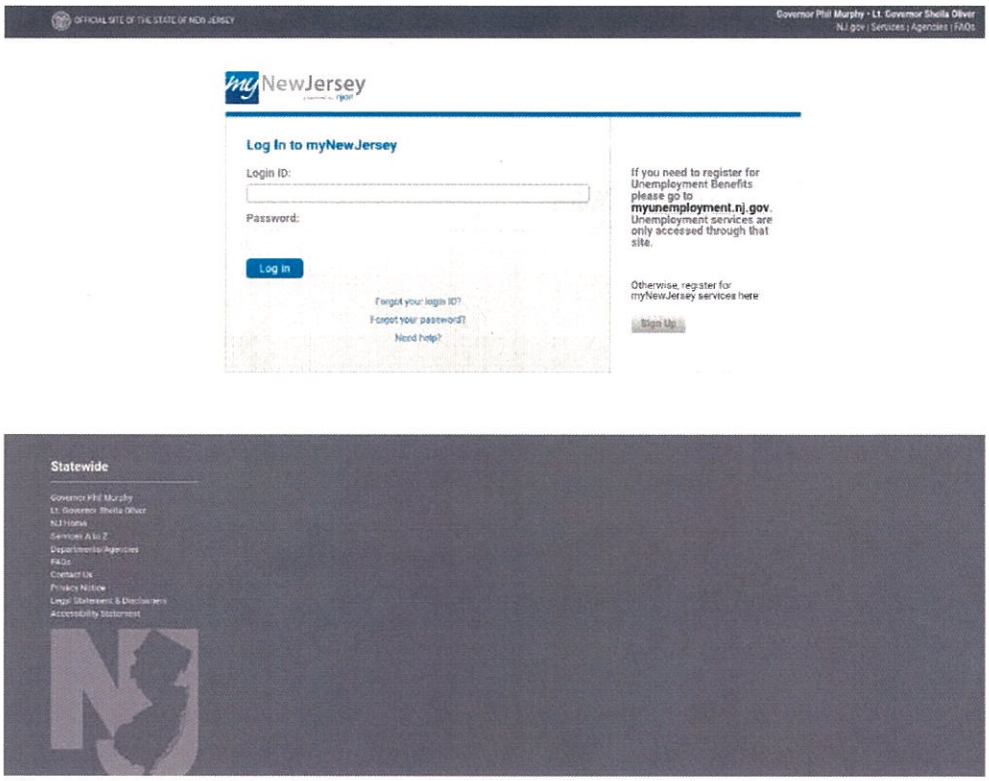
The PDF, if opened, displays myNewJersey branding and instructs the user to click on the "Open" link to view the document.

Continued on next page.

23x



The included link (hxxp://my-state-nj-us.plusandminues[.]com) redirects the user to another website (hxxp://cclifestyle[.]net/aul/login), which impersonates the official myNewJersey login page and requests the user's Login ID and Password.

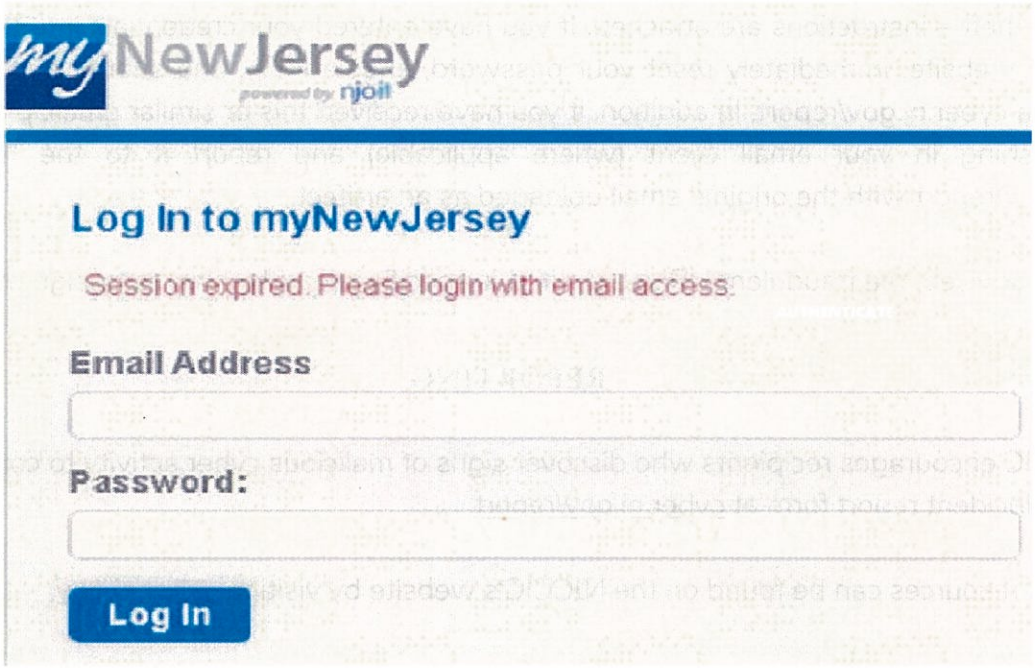


If submitted, the user receives an error notice of "Session expired. Please login with email access,"

Continued on next page.

24

and requests the user to enter their email address and corresponding password.



If submitted, the user is then redirected to the official NJ Division of Pensions & Benefits website in an effort to convince the user that their login simply failed.

If any information is submitted into these forms, they are sent to the threat actor(s) behind the spearphishing campaign. If you have not implemented multi-factor authentication (MFA) on your myNewJersey account, these credentials (username/email and password combinations) can be used to gain unauthorized access to the myNewJersey portal and access sensitive employee information, including MBOS. Using the information provided within the myNewJersey portal, threat actors can commit identity theft, such as filing fraudulent tax returns in order to steal tax refunds. Additionally, within the MBOS portal, threat actors can change beneficiary information, apply for pension loans, and submit applications for withdrawal. If the compromised password is also used for other online services, this could also provide the threat actor with unauthorized access to those accounts where MFA is not enabled.

Users are highly advised to refrain from clicking links or opening attachments delivered in emails from unverified senders and, instead, navigate directly to official websites – in this case,

Continued on next page.

25x

my.state.nj.us. Additionally, users are advised to ensure that multi-factor authentication has been enabled on their myNewJersey account in order to prevent unauthorized account access via credential theft – instructions are attached. If you have entered your credentials into this or other fraudulent website, immediately reset your password, enable MFA, and submit a report to the NJCCIC via cyber.nj.gov/report. In addition, if you have received this or similar email, please report it as phishing in your email client (where applicable) and report it to the NJCCIC via cyber.nj.gov/report with the original email uploaded as an artifact.

Please be advised, the fraudulent URLs used in this specific spearphishing campaign may vary.

REPORTING

The NJCCIC encourages recipients who discover signs of malicious cyber activity to contact us via the cyber incident report form at cyber.nj.gov/report.

Additional resources can be found on the NJCCIC's website by visiting cyber.nj.gov.

26x

DATA BREACH PREVENTION, RESPONSE, AND RESOURCES

Threat actors target valuable data, such as personally identifiable information (PII), protected health information (PHI), criminal justice information, student educational records, intellectual property, and financial and payment card information. If valuable data is insecure and accessible, it is a matter of when, not if, it is located and exposed. Cyber incidents continue to increase and, as a result, data breaches are unfortunately becoming the norm. Not all cyber incidents result in data breaches; however, all data breaches are a result of cyber incidents. In an effort to reduce the likelihood and impact of cyber incidents and prevent data breaches, it is important for organizations to prepare for and respond efficiently and effectively to cyber incidents, collaborate with law enforcement and intelligence agencies, report data breaches, and implement cybersecurity best practices.

INCIDENT RESPONSE

Incident response is critical in the event of a cyber incident. The National Institute of Standards and Technology (NIST) sets standards and practices for cybersecurity and responding efficiently and effectively to incidents as outlined in the four main phases of the NIST Incident Response Life Cycle:

(1) Preparation

- This initial phase involves establishing and training an incident response team and acquiring the necessary tools and resources. Preparation is the key to effective and rapid response to help limit the impact of cyber incidents. This phase includes compiling a list of all assets, creating a communication plan (describing who to contact and what to do), and creating an incident response plan. Controls should also be selected and implemented based on the results of risk assessments; however, residual risk will inevitably persist after controls are implemented. This phase should also include defining security events and their thresholds to be investigated.

(2) Detection and Analysis

- Detection is necessary to alert organizations whenever there are indications of a potential security incident. Accurately detecting and assessing incidents is often the most difficult part of incident response for many organizations.

27x

Continued on next page.

(3) Containment, Eradication, and Recovery

- This phase includes patching the threat's entry point, removing the threat, and ensuring systems are operational or back to business as usual. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. This phase also focuses on keeping the incident impact as minimal as possible and mitigating service disruptions. Activity may cycle back to the previous phase to see if additional incidents are detected while eradicating the initial incident.

(4) Post-Incident Activity

- After the incident is adequately handled and operations are back to normal, a review of the incident is just as important as the preparation. This phase includes conducting a root cause analysis of the incident and analyzing incident response efforts. It is important to understand why the incident happened, its impact, what actions were taken to mitigate it and resolve it, and what should be done to prevent or better respond to future incidents. Learning from the experience, identifying areas for improvement, and updating the documentation are some of the most important, yet most often ignored, parts of incident response.

Source: NIST

The incident response plan should be implemented, rehearsed, and tested regularly with critical stakeholders so that relevant parties are aware of their responsibilities and can respond properly o to minimize downtime and cost to the organization in the event of a cyber incident. Tabletop exercises are highly recommended to identify valuable data and critical assets, account for roles and responsibilities, review various scenarios, assess risk, and adjust any procedures and guidelines as necessary. Lastly, the incident response plan should be complete, sufficiently detailed, and current.

28x

Continued on next page.

CYBER INSURANCE

Cyber insurance has quickly become an essential resource for businesses. While having some form of cyber insurance in place can help an organization in the event of a cyber incident, an organization is also responsible for its own cybersecurity and the responsibility is not shifted to the insurer. Cyber insurance has emerged as a standalone line of coverage that can help mitigate losses from a variety of cyber incidents and its aftermath, including data breaches, business interruptions, and network damage. Large organizations may have coverage to transfer risk and costs associated with a data breach, whereas smaller organizations may not.

The cost of a cyber insurance policy will depend on a number of different factors including the size of the organization, annual revenue, the industry in which it operates, the sensitivity of data handled, and the overall security of the network. For example, underwriting data recovery and system forensics would help cover some of the cost of investigating and remediating a cyber incident by employing forensic cybersecurity professionals to aid in discovering attack vectors and remediation of vulnerabilities. In the case of ransomware, some insurance companies also cover the cost of paying the ransom, despite guidance from law enforcement and the information security community. The insurance company looks at what the potential incident response and forensic bill might be. Unfortunately, this bill will be more costly in most cases as many organizations are not prepared and, therefore, insurance companies would rather pay the ransom.

Organizations will need to make sure they understand what is covered and, perhaps more importantly, what is not covered when agreeing to a coverage policy. Plans may not cover legal costs or penalties. There may also be an additional deductible not covered in the overall costs. Depending on several factors—such as disclosure requirements, the size of the breach, and other things hiding in the fine print—that damage can be considerable. Therefore, organizations should ensure they know exactly what their cyber insurance policy covers and understand the potential costs of the most likely cyber incidents, such as ransomware.

COLLABORATIVE EFFORTS WITH LAW ENFORCEMENT AND INTELLIGENCE AGENCIES

Reporting cyber incidents to law enforcement is becoming a common requirement for insurance companies, and is also beneficial to organizations by providing guidance and access to additional resources. In the event of a law enforcement cyber investigation, remediation of the incident will not be hindered nor will the organization be forced to halt their operations.

Cyber incidents can also be reported to intelligence agencies, such as the NJCCIC via the Cyber

29x

Continued on next page.

Incident Form, in an effort to bridge the information sharing gaps between local, state, federal, public, and private sector organizations to reduce cyber risk and respond to emergent incidents. Organizations may not be aware of specific threats, trends, suspicious indicators, or vulnerabilities. Organizations willing to provide incident details—such as attack vectors, vulnerabilities exploited, and tactics used—will assist others in increasing their resiliency to these various threats.

MANDATORY DATA BREACH REPORTING

Organizations have an obligation to protect information and report a breach of security. According to the New Jersey Identity Theft Prevention Act, a "breach of security" is defined as the "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality, or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable." Furthermore, any organization that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, are required to disclose any breach of security of those records following discovery or notification of the breach to any New Jersey resident whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

Organizations are mandated by law to report data breaches and the NJCCIC provides the reporting mechanism for data breaches via the State of New Jersey Data Breach Report Form. When filing a data breach report, organizations are required to provide data breach details, including the number of NJ residents affected, data compromised (including PII), and consumer notification. Once submitted, it is reported to the NJCCIC for intelligence purposes, the NJ State Police for possible criminal activity, and the NJ Office of Attorney General for consumer impact. For more information and questions on data breaches, the law, and reporting, please contact the NJ Office of the Attorney General, Office of Consumer Protection.

In the event of a data breach, organizations should communicate and report information in a timely, accurate, and transparent manner to impacted business partners, regulators, and/or consumers. After a breach is discovered, organizations typically issue a public statement and offer a free comprehensive package of identity theft protection and credit file monitoring. If it is suspected that personally identifiable information (PII) has been compromised, impacted consumers are advised to review the NJCCIC Informational Report Compromised PII: Facilitating Malicious Targeting and Fraudulent Activity for recommendations and resources, including information on credit freezes and enabling multi-factor authentication (MFA) on accounts.

30x

Continued on next page.

CYBERSECURITY BEST PRACTICES

The NJCCIC provides individuals and organizations with information and resources for cybersecurity best practices and implementing preventive measures to help protect themselves from cyber incidents and data breaches. The NJ Statewide information Security Manual (SISM) includes a set of policies, standards, procedures, and guidelines. It sets a clear direction for information security, and it also provides effective management of risk and ensures the confidentiality, integrity, and availability of information and information systems. It has been derived from State and federal laws, industry best practices, and lessons learned, along with New Jersey State Government business and technology-related considerations. Additionally, the NJCCIC Cybersecurity Program Controls Assessment, which is aligned with the NJ SISM, covers many control areas and helps organizations understand their own cybersecurity program and identify risks and establish strategies and tactics to manage them. The Assessment can be obtained by emailing the NJCCIC at njccic@cyber.nj.gov.

For more cybersecurity information, please visit our website at cyber.nj.gov.

31x

NJCCIC WEEKLY BULLETIN

MARCH 17, 2022

GARDEN STATE CYBER THREAT HIGHLIGHTS

Russia/Ukraine Cyber Threat Update

At this time, the NJCCIC is not aware of any specific or imminent cyber threats to NJ. However, as sanctions against Russia take effect, it is increasingly likely that there will be retaliatory cyber activity against the West. As such, the cyber threat level in NJ was raised to ELEVATED, which indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service. At this level, there are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high. Please refer to the latest NJCCIC Advisory and the Cybersecurity and Infrastructure Security Agency's Shields Up website for the latest risk mitigation practices.

Ukraine Donation Scams Continue

The NJCCIC previously reported about scams exploiting attempts to provide assistance to the people of Ukraine, including fraudulent websites requesting donations in the form of cryptocurrency. This week, we continue to see similar scams and identified a fraudulent donation website. The legitimate looking website requests cryptocurrency and includes a tally of incoming donations from various cryptocurrency wallet addresses, which was determined to be fake after analysis. As the NJCCIC identifies scam websites, we submit cease and desist requests to the website's registrar and/or hosting provider, though this process can take some time.

The NJCCIC recommends users and organizations educate themselves and others on these continuing threats and tactics to reduce victimization. We advise users to research and make donations to only reputable, known, and verified websites/charities, and identify whether the charity has already established a presence in Ukraine as not all relief organizations will be able to provide timely assistance. These types of scams may be reported to the FTC, FBI's IC3, the associated platform, and the NJCCIC.

Cyber Threat Actors Employed Thread Hijacking to Target Contacts from Stolen Email Data

Continued on next page.

324

The NJCCIC was made aware of tactics used in social engineering schemes initiated after a network compromise. In many of the initial compromises, email exchange servers were hacked and data, including email threads and contacts, were stolen. Using this information, the threat actors distributed spearphishing emails using thread hijacking – a technique in which malicious messages are sent within existing conversations. While these messages are often sent from unassociated email accounts, the threat actors employ display name spoofing to appear as though the communication is coming from one of the contacts in the email thread. The combination of contact impersonation and use of existing conversations lends a perceived legitimacy to the email, which increases the likelihood of success in convincing the email recipient to take the threat actor's desired action – such as opening an attachment, clicking a link, transferring funds, or divulging sensitive information. These same tactics are also used in cyber threat activity subsequent to email account compromises, indicating that the emails sent by the threat actors are from legitimate accounts and require additional attention to determine their illegitimacy.

The NJCCIC highly advises organizations and businesses that have experienced a network compromise to evaluate whether data was exfiltrated and, if so, what data was stolen. Additionally, include external message warnings in emails originating outside of your organization to signal to users that they should exercise caution with the communication. Users are encouraged to increase their awareness of the tactics employed by threat actors in social engineering schemes so that they may identify these attempts and prevent victimization.

Emotet Activity Increases Rapidly, Attempts to Install Via IRS Impersonation Phishing Campaigns

Emotet attempts to infect via various phishing campaigns, including several that impersonate the IRS and request the potential victim to open the included attachment, which is often password protected. The email, however, includes the password to open the attachment. The ZIP file contains an Excel attachment that, if opened, requests the user to Enable Editing then Enable Content. Enabling content permits macros to run, allowing Emotet to be installed on the system. Some red flags included in the phishing email are noted in the image above and include display name spoofing and misspellings. While this campaign impersonates the IRS, Emotet threat actors impersonate various other known organizations in order to emit a sense of authority and legitimacy with their potential victims.

The NJCCIC advises users to refrain from clicking links, opening attachments, or enabling macros

Continued on next page.

33x

in communications received from unknown or unverified senders and exercise caution with those from known senders. Additionally, maintain awareness of common red flags and tactics used by cyber threat actors in social engineering campaigns such as phishing emails. Network defenders are encouraged to establish policies that prevent macros from running in Microsoft documents and establish a defense-in-depth cybersecurity strategy that uses layered defenses to thwart malware infections, such as Emotet.

THREAT ALERT

Malicious Cyber Activity Targeting Smartphones

Smartphones are an integral part of daily life, both for personal and professional use. However, as smartphone use continues to increase, they become attractive targets for cyber threat actors. Many of us are continuously connected to the internet and able to check our email and social media, and navigate the web on the go. The size of smartphones and the apps available on them, however, make it inherently more difficult to identify potentially malicious emails, messages, and websites. In an effort to fit content on our screens, valuable information is sometimes discarded. For example, email applications often only show email sender display names – which can be easily modified – and leave out the sender's corresponding email address. This makes identifying impersonation phishing emails more difficult and can lead to higher rates of victimization. The same is true for web browser applications that do not fully display some website URLs, which could allow duplicated websites to go unnoticed. In addition to email, phishing messages are also distributed via SMS text – a tactic dubbed "SMiShing." These messages often claim to be delivered from known contacts or companies and include malicious links meant to steal information or distribute malware.

The NJCCIC advises smartphone users to exercise caution when using their devices, ensuring that communications are coming from legitimate entities and that they are visiting official websites. Additionally, avoid clicking links or opening attachments in messages from unknown senders, and navigate directly to websites in lieu of clicking links. Further information on the targeting of smartphones and recommendations to reduce risk can be found in the ZDNet article and NJCCIC post Mobile Device Security.

VULNERABILITY ADVISORIES

Continued on next page.

34x

QNAP NAS Devices Impacted by "Dirty Pipe"

QNAP is notifying users that Network Attached Storage (NAS) devices are impacted by the high severity Linux vulnerability dubbed "Dirty Pipe " that allows attackers with local access to gain root privileges. Proof of Concept (PoC) exploits have been made publicly available. Although a patch was released for the flaw, QNAP states that there is no mitigation available at this time, further recommending that users install the security updates as soon as possible. Impacted NAS devices comprise of those running QTS 5.0.x and QuTS hero h5.0.x, including: QTS 5.0.x on all QNAP x86-based NAS and certain QNAP ARM-based NAS; and QuTS hero h5.0.x on all QNAP x86-based NAS and certain QNAP ARM-based NAS.

The NJCCIC recommends QNAP NAS users and administrators apply updates as soon as possible after appropriate testing and apply the following recommendations: avoid exposing NAS device to the internet, however, if this is not possible, disable the Port Forwarding function of the router; and consider disabling the UPnP function of the QNAP NAS. Further recommendations can be found in the QNAP security advisory.

High Severity Kubernetes Vulnerability Patched

CrowdStrike security researchers discovered a high severity vulnerability, dubbed "cr8escape," in the Kubernetes container engine CRI-O – an open source, community-driven container engine. Each Kubernetes node includes a container runtime such as CRI-O. Among other tasks, the container runtime allows containerized apps to safely share each node's underlying Linux kernel and other resources. The flaw, tracked as CVE-2022-0811 (CVSS v3 8.8), exists due to the addition of sysctl support in version 1.19 used to configure kernel parameters at runtime. Researchers determined that this flaw will now "blindly set any kernel parameters it is passed without validation, meaning that anyone who can deploy a pod on a cluster using the CRI-O runtime can abuse the kernel.core_pattern parameter to achieve container escape and arbitrary code execution as root on any node in the cluster." Malicious threat actors may be able to exploit the vulnerability in the components of the Kubernetes architecture, such as the control plane, worker nodes, or containerized applications, to exfiltrate data and move laterally across pods. The potential impact of this flaw is widespread due to the number of platforms that use CRI-O, such as OpenShift and Oracle Container Engine for Kubernetes. The vulnerability has been resolved and researchers urge users to patch immediately.

The NJCCIC recommends users and administrators to apply updates immediately after

Continued on next page.

35x

appropriate testing. Additionally, apply hardening procedures found in CISA's and NSA's Kubernetes Hardening Guide. Further remediations and technical details can be found in the CrowdStrike blog post.

REPORTING

The NJCCIC encourages recipients who discover signs of malicious cyber activity to contact us via the cyber incident report form at cyber.nj.gov/report.

Additional resources can be found on the NJCCIC's website by visiting cyber.nj.gov.

36x

RANSOMWARE: RISK MITIGATION STRATEGIES

TLP: WHITE | While ransomware infections are not entirely preventable due to the effectiveness of well-crafted phishing emails and drive-by downloads from otherwise legitimate sites, organizations can drastically reduce this risk by implementing cybersecurity strategies and improving cybersecurity awareness and practices of all employees. The most effective strategy to mitigate the risk of data loss resulting from a successful ransomware attack is having a comprehensive data backup process in place; however, backups must be stored off the network and tested regularly to ensure integrity. To increase the likelihood of preventing ransomware infections, organizations must conduct regular training exercises and awareness briefings with all employees to ensure understanding of safe-browsing techniques and how to avoid phishing attempts. The following is a comprehensive list of recommendations, though not exhaustive, to reduce the risk posed by ransomware infections:

DATA PROTECTION

- Schedule backups of data often and ensure they are kept offline in a separate and secure location. Consider maintaining multiple backups in different locations for redundancy. Test your backups regularly.
- If an online backup and recovery service is used, contact the service immediately after a ransomware infection is suspected to prevent the malware from overwriting previous file versions with the newly encrypted versions.

SYSTEM MANAGEMENT

- Ensure anti-virus software is up-to-date with the latest definitions and schedule scans as often as permitted.
- Enable automated patching for operating systems, software, plugins, and web browsers.
- Follow the Principle of Least Privilege for all user accounts and enable User Access Control (UAC) to prevent unauthorized changes to user privileges.
- Implement application whitelisting to prevent unauthorized or malicious software from executing.
- Turn off unused wireless connections.
- Disable macros on Microsoft Office software.

Continued on next page.

37x

- Use ad blocking extensions in browsers to prevent "drive-by" infections from ads containing malicious code.
- Disable the vssadmin.exe tool by renaming it to prevent ransomware from deleting Shadow Volume Copies.
- Disable Windows Script Host and Windows PowerShell.
- Disable Remote Desktop Protocol (RDP), Telnet, and SSH connections on systems and servers if it is not needed in your environment. Block inbound traffic to associated ports.
- If remote access is needed, audit access, ensure that login credentials are complex, and implement a 2FA solution to prevent unauthorized access.
- Use web and email protection to block access to malicious websites and scan all emails, attachments, and downloads and configure email servers to proactively block emails containing suspicious attachments such as .exe, .vbs, and .scr.
- Configure systems by modifying the Group Policy Editor to prevent executables (.exe, .rar, .pdf., exe, .zip) from running in %appdata%, %localappdata%, %temp% and the Recycle Bin. CryptoPrevent is a free tool that can help automate this process and prevent ransomware from executing.
- Implement a behavior blocker to prevent ransomware from executing or making any unauthorized changes to systems or files.
- Consider utilizing a free or commercially available anti-ransomware tool by leading computer security vendors.
- To counteract ransomware variants that modify the Master Boot Record (MRB) and encrypt the Master File Table (MFT), Cisco Talos has released a Windows disk filter driver called MBRFilter.
- For Mac OS X users, consider installing the free tool, RansomWhere?. Information about this tool is available on the Objective-See website.

NETWORK MANAGEMENT

- Ensure your firewall is enabled and properly configured.
- Close and monitor unused ports.
- Disable SMBv1 on firewall and all systems on the network.
- Block inbound traffic to TCP/UDP ports 139 and TCP port 445.
- Block known malicious Tor IP addresses.
- Set a network performance baseline for network monitoring prior to an infection to make looking for anomalies and malicious activity easier after the infection.

Continued on next page.

38x

- After removing the malware or restoring the machine, make sure to change all system, network, and online account passwords and implement the mitigation recommendations provided in this document.

REPORTING

If you or someone in your organization is the victim of a ransomware infection, or would like to learn more about the NJCCIC, please visit cyber.nj.gov, email njccic@cyber.nj.gov, or call 1-888-4-NJCCIC.

- Keep network log files for a full year in the event a ransomware or other network intrusion incident leads to a criminal investigation.

MOBILE DEVICE MANAGEMENT

- For Apple iOS devices: ensure data is backed up on iCloud and two-factor authentication is enabled, only download media and apps from the official iTunes and App Stores, and avoid "jailbreaking" the device.
- For Android devices: disable the "unknown sources" option in the Android security settings menu, only install apps from the official Google Play store, and avoid "rooting" the device.

HOW TO LIMIT THE IMPACT OF RANSOMWARE INFECTIONS

- All employees should be instructed to immediately unplug the Ethernet network cable or disable Wi-Fi on the system if they suspect a ransomware infection has initiated. This will prevent the ransomware from spreading to other devices on the network or infecting backups that are stored on the network or in a cloud environment. Do not reconnect until the computer or device has been thoroughly scanned and cleaned.
- Alternatively, instruct employees to turn off the power or unplug the power cord from the system. Although doing so inhibits complete forensic analysis of the infected device, it stops the encryption process and may limit data loss.
- Employees should notify the appropriate information security contact within your organization as quickly as possible.

HOW TO RECOVER AFTER A RANSOMWARE INFECTION HAS OCCURED

- Are there complete backups for the affected data or system that predate the infection (to avoid restoring an infected instance)? If so, restore from backups and take steps to prevent future infections.
- If not, is there a publicly available decryption tool or remediation method? Refer to the NJCCIC's Ransomware Threat Profile for a comprehensive list of ransomware variants and those with known decryption tools.
- If no decryption tool is available, the only remaining options are to accept the loss or pay the ransom. The NJCCIC discourages paying ransoms of any kind, as this perpetuates the crime and does not guarantee recovery of data.

Continued on next page.

39x

New Jersey Cybersecurity & Communications Integration Cell

The New Jersey Cybersecurity and Communications Integration Cell is the state's one-stop shop for cybersecurity information sharing, threat intelligence, and incident reporting. Acting in a cyber fusion center capacity, the NJCCIC is a component organization within the New Jersey Office of Homeland Security and Preparedness. It is comprised of staff from NJOHSP, the New Jersey Office of Information Technology, and the New Jersey State Police. The NJCCIC mission is to make New Jersey more resilient to cyberattacks by promoting statewide awareness of cyber threats and widespread adoption of best practices.

NJCCIC SERVICES

As individuals, businesses, schools, and government agencies continue to expand their online footprints, they are more exposed to cyberattacks. The NJCCIC provides a wide array of cybersecurity services, including the development and distribution of cyber threat intelligence products, alerts, and advisories, as well as cyber tips and best practices for effectively managing cyber risk.

INCIDENT REPORTING

The NJCCIC partners with the New Jersey State Police Cyber Crimes Unit, the Federal Bureau of Investigation, and the US Department of Homeland Security to assist victims in responding to and recovering from cybersecurity incidents, and to prevent future attacks. We encourage all New Jersey citizens and organizations to report cyber incidents and data breaches.

- To file a cyber incident report, visit cyber.nj.gov/report
- To file a data breach report, visit cyber.nj.gov/breach

MEMBERSHIP

Individuals and organizations wishing to receive alerts, advisories, bulletins, and more can register to become an NJCCIC member at no cost. An NJCCIC membership enables you to increase your knowledge and awareness, becoming the strongest defense against cyber-attacks. Sign up on our website by visiting cyber.nj.gov/membership.

CONTACT US

Business Hours: M-F, 8am-5pm
Phone: 1-833-4-NJCCIC (833-465-2224)
24/7 Hotline: 1-866-4-SAFE-NJ (866-472-3365

CONNECT WITH US

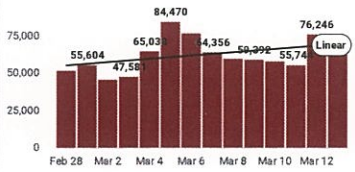
For the latest news, updates, and alerts, follow the NJCCIC on Twitter @NJCybersecurity and on Facebook at facebook.com/NJCCIC.

Threat Activity from Geopolitical Hotspots

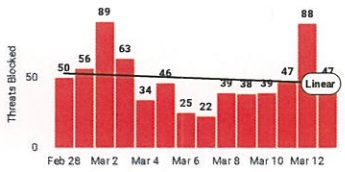
March 18, 2022

Russia: Past Week	Belarus: Past Week	Iran: Past Week	China: Past Week
442,155	268	131,016	590,363
▲ 4% Compared to Previous Week	▲ 18% Compared to Previous Week	▲ 7% Compared to Previous Week	▲ 0% Compared to Previous Week
51,374	37	11,853	73,085
Russia: Past Day	Belarus: Past Day	Iran: Past Day	China: Past Day
▲ 3% Compared to Previous Day	▲ 61% Compared to Previous Day	▲ 2% Compared to Previous Day	▲ 3% Compared to Previous Day

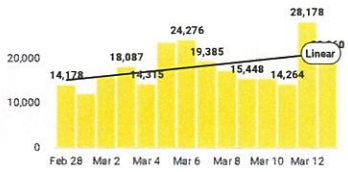
Russia: Daily Trend



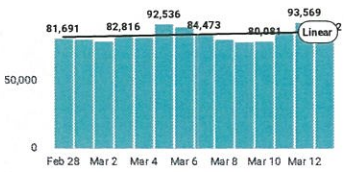
Belarus: Daily Trend



Iran: Daily Trend

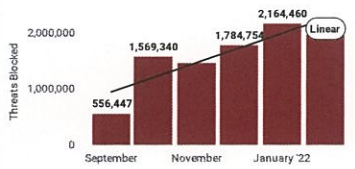


China: Daily Trend

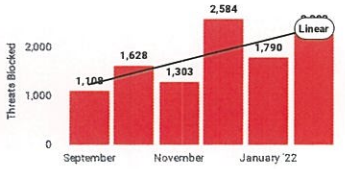


Russia: Past Month	Belarus: Past Month	Iran: Past Month	China: Past Month
2,164,460	2,383	537,550	2,312,783
▲ 10% Compared to Previous Month	▲ 33% Compared to Previous Month	▼ -18% Compared to Previous Month	▲ 1% Compared to Previous Week

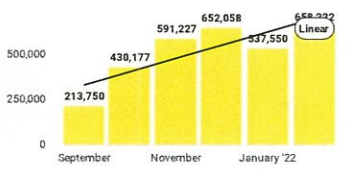
Russia: Past 6 Months



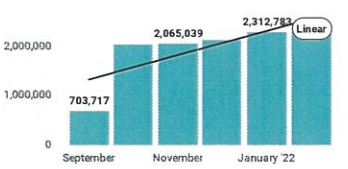
Belarus: Past 6 Months



Iran: Monthly View



China: Past 6 Months



83,064,530

Total Threats Blocked - All Countries - Past Month

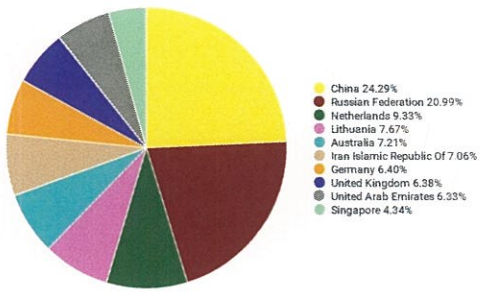
▲ 6% Compared to Previous Month

12,780,864

US: Past Month

▲ 22% Compared to Previous Month

Top 10 International Countries (% Threats Blocked)



For further information on this report, please contact the:

New Jersey Cybersecurity & Communications Integration Cell
24/7 Incident Reporting: 1.866.4.SAFE.NJ
General Inquiries: 1.833.4.NJCCIC
www.cyber.nj.gov

45x

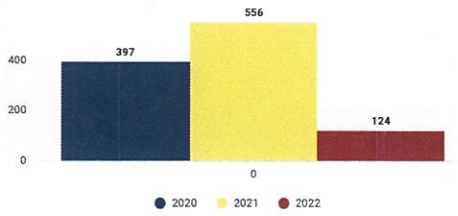
NJCCIC Overview

Cyber Incidents Reported to the NJCCIC

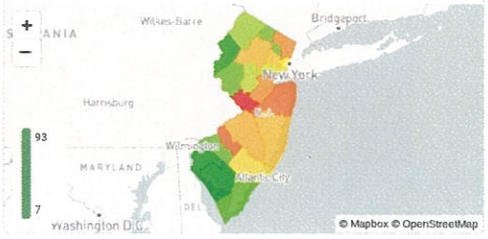
124

Cyber Incidents Reported to the NJCCIC: 2022

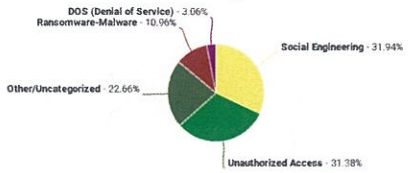
Cyber Incidents Reported to NJCCIC: 2020-2022



Counties from which Reports were made



Incident Types



Incident Types (Year over Year)

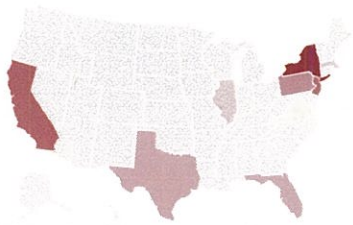
Case Created Year	2020	2021	2022
Incident Type Groups	# Incidents	# Incidents	# Incidents
Other/Uncategorized	135	83	26
Social Engineering	99	191	54
Unauthorized Access	91	210	37
Malware/Ransomware	57	54	7
DOS (Denial of Service)	15	18	

Data Breaches Reported to the NJCCIC

Data Breaches by Year: 2020-Present

Year	No. Data Breaches	No. NJ Residents Affected
2022	398	240,876
2021	1,877	2,989,000
2020	1,479	1,949,688

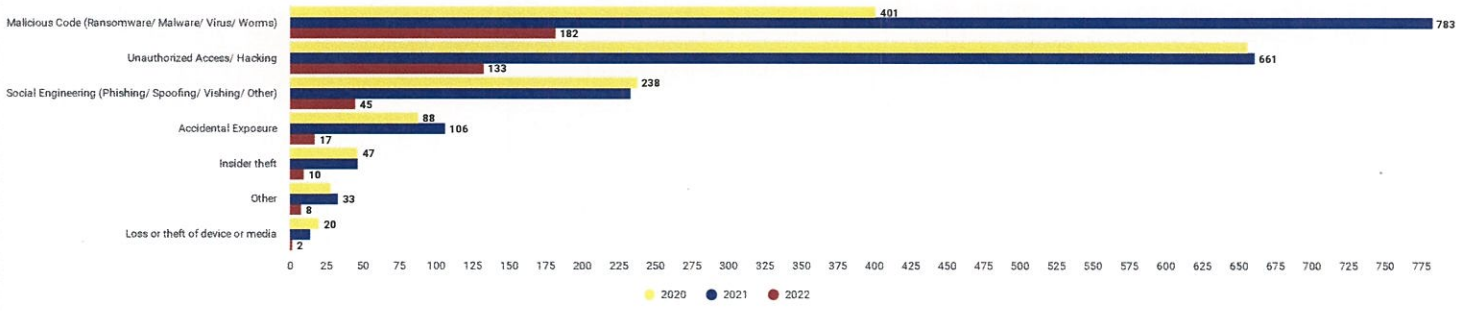
Locations of Reporting Organizations



Data Breaches by Organization Type (Top 10)

Organization Type	Breaches Reported: 2020-2022
Finance and Insurance	914
Other Services (except Public Administration)	531
Professional, Scientific, and Technical Services	429
Health Care and Social Assistance	423
Educational Services	325
Retail Trade	296
Manufacturing	224
Arts, Entertainment, and Recreation	94
Accommodation and Food Services	82
Transportation and Warehousing	66

Data Breach Causes: 2020 - Present



NJCCIC Membership

11,901

NJCCIC Members

Members by Sector

Sector	Members
Government Facilities	3,618
Emergency Services	1,493
Information Technology	1,084
Financial Services	706
Healthcare and Public Health	504
Commercial Facilities	257
Water and Wastewater Systems	188
Energy	175
Communications	153
Transportation Systems	139

NJCCIC Membership - Top 10 Countries

Country	# of Members
United States	11,664
India	39
Canada	26
United Kingdom	21
Australia	21
France	10
Israel	10
Germany	7
Singapore	7
Italy	6