



Defending Our Digital Density.



@NJCybersecurity



cyber.nj.gov



NJCCIC@cyber.nj.gov





NJCCIC

New Jersey Cybersecurity and Communications Integration Cell

The State's clearinghouse for information sharing, threat intelligence, best practices, and incident response

- Consists of OIT, NJSP, OHSP and Federal Partners
- All Threats/ All Hazards
- Promote statewide awareness of cyber threats
- Facilitate widespread adoption of best practices
- Develop public and private sector partnerships with the goal of making NJ more resilient to cyber attacks



Cyber Threat Landscape

- **Threat environment is increasing**
- **Growing dependence on technology and devices/systems results in increase of attack surface**
- **Bar to carry out crippling attacks is low**
- **Locally ubiquitous nature of Internet**
- **Top Threat Vectors:**
 - Email – phishing/malspam
 - Credential Harvesting
 - Infrastructure and application vulnerabilities

CNBC

Louisiana declares state of emergency after cybercriminals attack school districts

In a first for Louisiana, the governor has declared a state of emergency over a cybersecurity issue after a series of attacks on school districts and ...

Chicago Tribune

Illinois election officials say hack yielded information on 200,000 voters

Illinois election officials say hack yielded information on 200,000 voters. The online voter registration portal was restored late last week, but the board has ...

RU Daily Targum

Former Rutgers student to pay \$8.6 M. for DDoS attacks against ...

Two years ago, Jha conspired with Josiah White of Washington, Pa., and Dalton Norman of Metairie, La. to create the "Mirai botnet," which shut down websites ...

Wall Street Journal

Cyberattacks Raise Alarm for U.S. Power Grid

Cyberattacks that have knocked out electric utilities in recent years, including one suspected hack earlier this month, have renewed concerns about computer criminals ...

TechCrunch

Equifax breach was 'entirely preventable' had it used basic security measures, says House report

A House Oversight Committee report out Monday has concluded that Equifax's security practices and policies were sub-par and its systems were old and ...

Cyberattack Treated as a Statewide Emergency in Colorado

Looking back at the SamSam Ransomware attack of February 2018 on the Colorado ...

Cyberattack 'crippling' for Georgia courts

... they demanded a ransom by using a ransomware identified as ...

NJ.com

Stevens Tech struggling to rebound from cyberattack in ...

Stevens Tech struggling to rebound from cyberattack in time for start of school year ... Involved ransomware, but "Stevens took immediate action to preserve and ...

Wall Street Journal

Cybersecurity

Major cities have some form of smart-technology program, including automated traffic-control systems and ...

CBS News

Ex-Mossad director says cyber attacks pose biggest threat to free world

"I believe [cyber] is the biggest threat that the free world, our planet, is dealing with these days," Pardo said, calling cyber attacks a "soft and silent nuclear ...

The Texan

Governor Abbott Orders State Resources on Standby as ...

On Monday, Governor Greg Abbott ordered state resources to be placed on standby. The Texas Department of Emergency Management will be deploying Texas ... she worked as a Cyber Security Consultant

Fortune

Baltimore's Ransomware Mess Is Its Own Fault—Cyber Saturday

Since early May, Baltimore has been grappling with a city-crippling ransomware ... WannaCry and Russia's NotPetya—costing billions of dollars in damages for ...

Ars Technica

Rash of ransomware continues with 13 new victims—most of them schools

The ransomware involved in the Texas attacks, which hit 22 local-level ... because of their low budget for information technology and limited security resources.

CNBC

Email wire fraud is so simple for criminals to pull off, it's cost companies \$26 billion since 2016, says FBI

A type of wire fraud called "business email compromise" is growing in prominence and is almost impossible to stop, resulting in losses of \$26 billion in the last ...

Yahoo Finance

Jamie Dimon: Cybersecurity threats may be the 'biggest threat to the U.S. financial system'

JPMorgan Chase (JPM) CEO Jamie Dimon has singled out cybersecurity as the "biggest threat" to the financial services industry. In his widely read annual letter, ...

Common Threats/Uncommon Impacts



"Think Like a Criminal"

POSSIBLE ACTORS



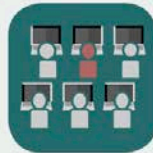
Nation-State
Actors



Criminals



Black Hat
Hackers



Insiders



Terrorists



Politically
Motivated
Groups

POSSIBLE MOTIVATIONS



Financial
Gain



Retribution
for
Perceived
Grievances



Fame and
Reputation



Sow Social
Division



Foment
Chaos /
Anarchy



Subvert
Political
Opposition



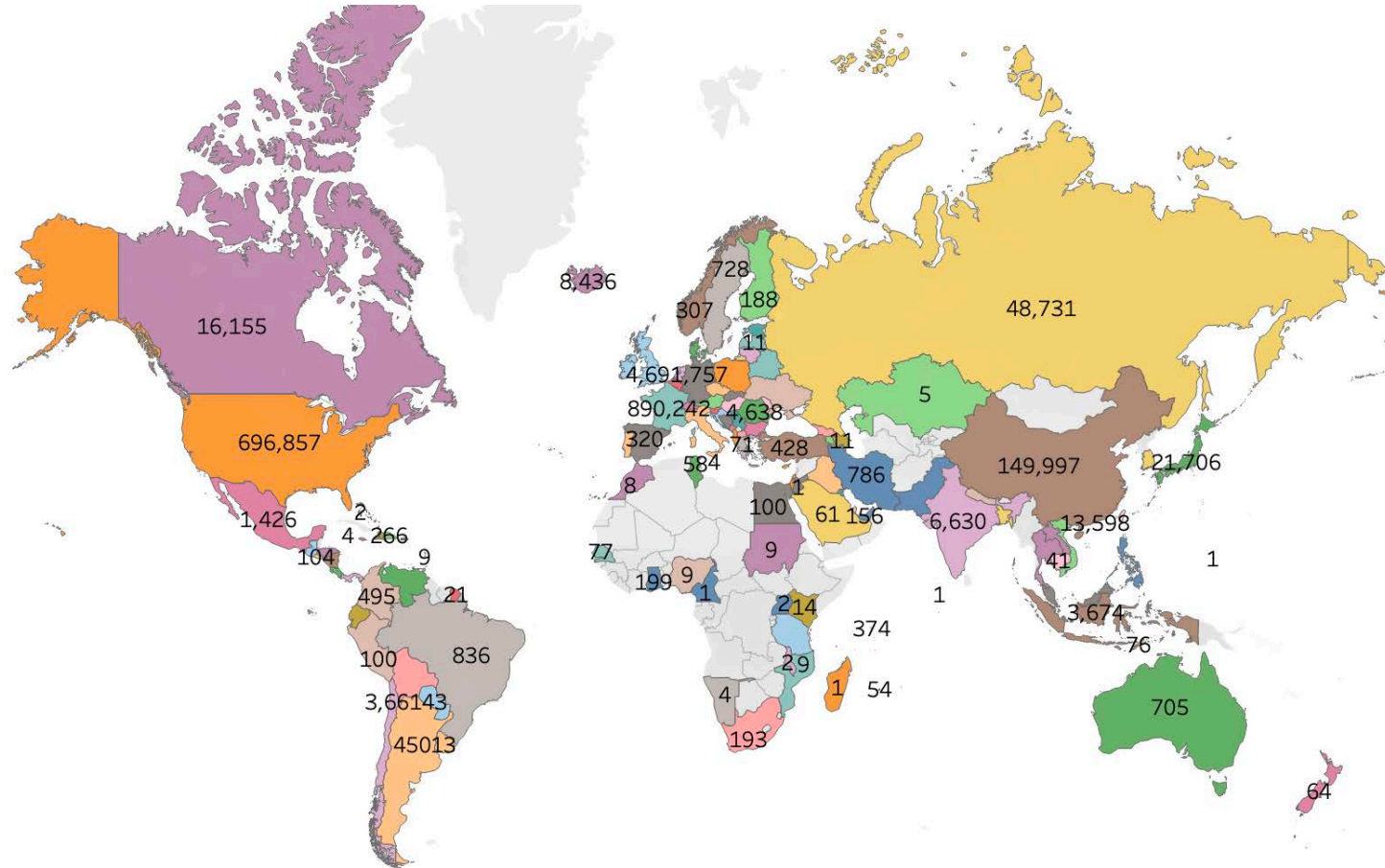
Foreign
Policy /
National
Interests



Undermine
Trust in
Democracy



Attacks Against Garden State Network



NJCCIC Weekly Bulletins and Alerts



NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

February 21, 2019

TLP: WHITE

Garden State Cyber Threat Highlight

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

Emotet, the Threat that Keeps on Giving

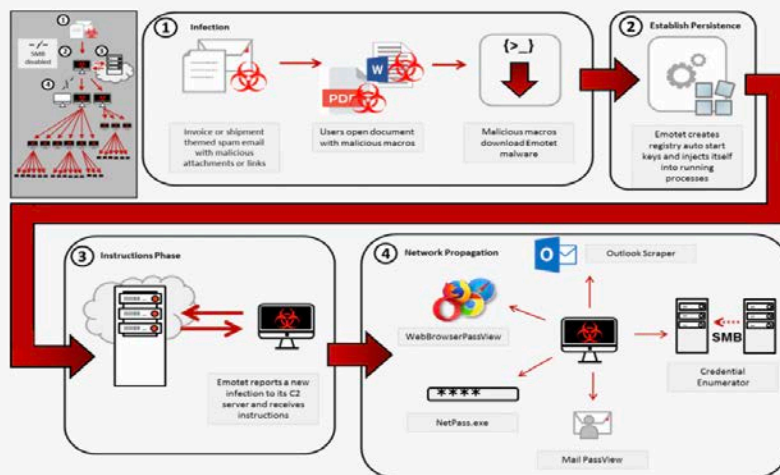


Image Source: US-CERT

Throughout 2018, and now into 2019, the [Emotet](#) trojan has been a prevalent cyber threat across New Jersey. The NJCCIC has received numerous reports regarding Emotet infections, often impacting the



NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

September 26, 2019

TLP: WHITE

Garden State Cyber Threat Highlight

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

Gift Card Scams Continue

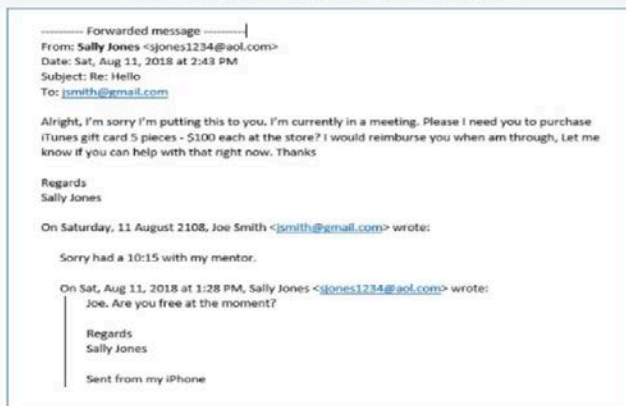


Image Source: APA

The NJCCIC continues to receive incident reports from New Jersey businesses, organizations, and citizens regarding gift card scams. Oftentimes, individuals receive an email with spoofed sender information to appear as though the email is coming from someone they know, most often a boss or colleague at work. The email urgently requests the recipient to purchase gift cards and instructs them



NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

April 4, 2019

TLP: WHITE

Garden State Cyber Threat Highlights

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

Extortion Scams Continue



The NJCCIC continues to receive reports of extortion scams, similar in nature, submitted by individuals throughout New Jersey. The threat actor sends emails to the target claiming they compromised the target's email account and computer, and then used their webcam to record them visiting adult content websites. The threat actor attempts to convince the target of the email's validity by including one of the target's legitimate passwords, which is most likely obtained from previous breaches in which this information was exposed and not a result of compromising the target's computer. In addition, they claim they have access to the target's contacts and will send the video to



NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

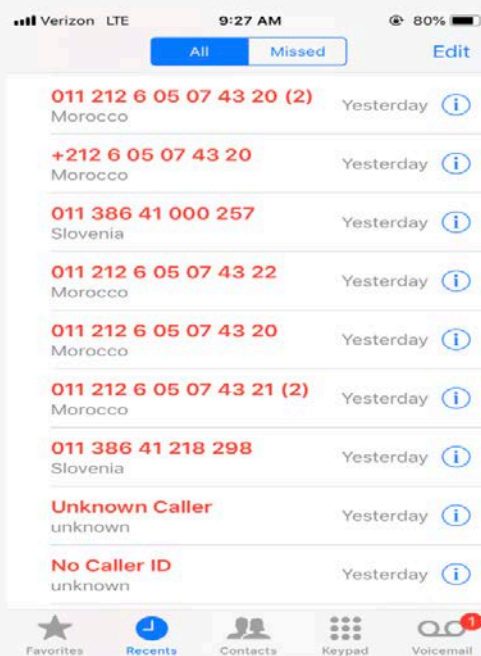
NJCCIC Alert

One Ring Phone Scam Continues

TLP: WHITE

March 22, 2019

NJCCIC Members,





NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

March 21, 2019

TLP: WHITE

Garden State Cyber Threat Highlight

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

BEC Campaign Attempts to Change Direct Deposit Information



The NJCCIC has received numerous incident reports from educational organizations around the State impacted by various business email compromise (BEC) campaigns involving direct deposit scams. Unlike phishing scams, BEC campaigns are a highly targeted form of social engineering. Threat actors commonly spoof the source name or email address of a familiar contact, use email domains that mimic

Credential Compromise

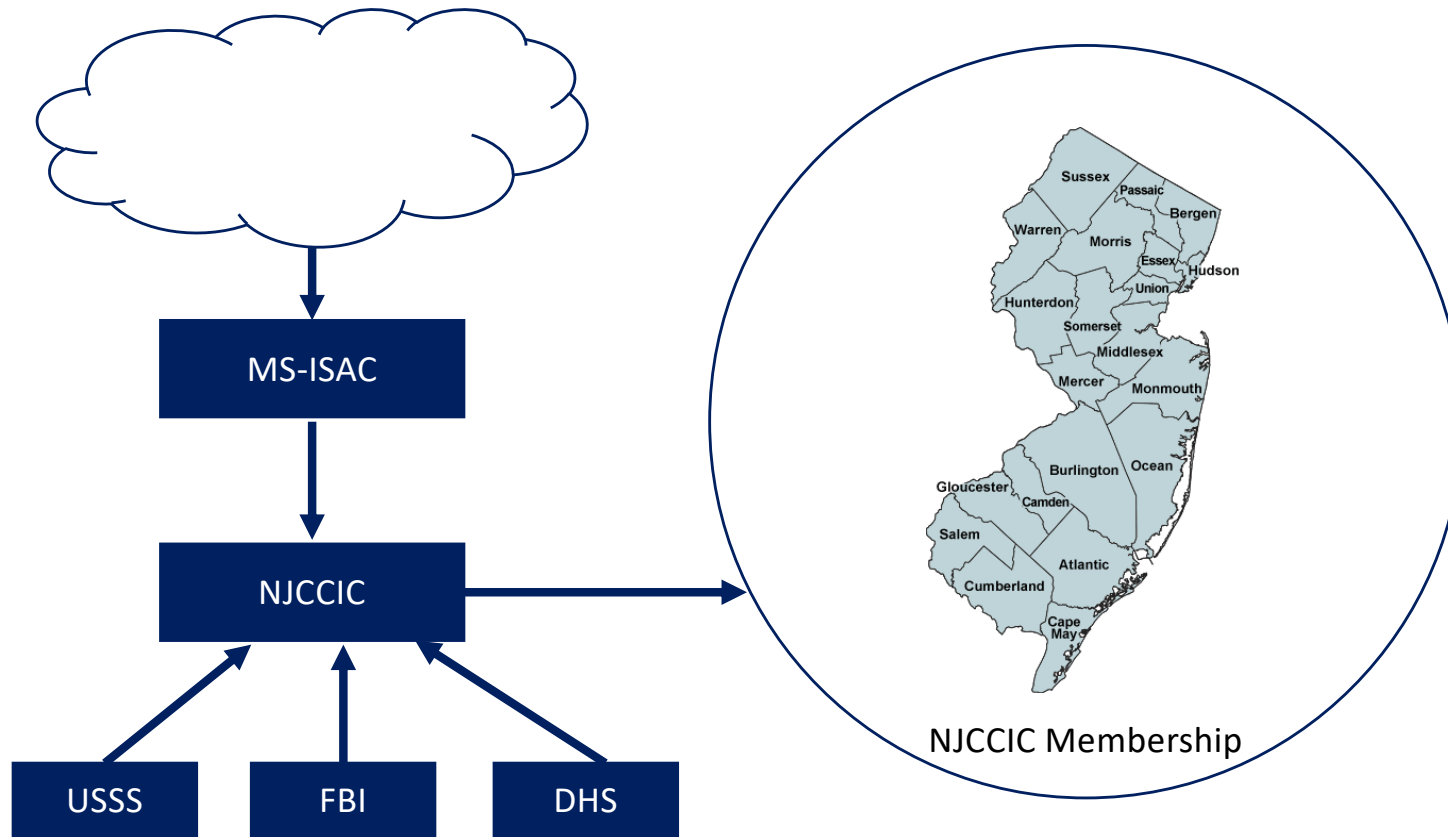


Credential Compromise

- Credentials are the keys to the kingdom
- Less than 35% of users have unique passwords across sites
- 28% of organizations provide multi-factor authentication (MFA)
- 78% of users within organizations that provide MFA hate it
- Privileged access: "Do as I say, not as I do"

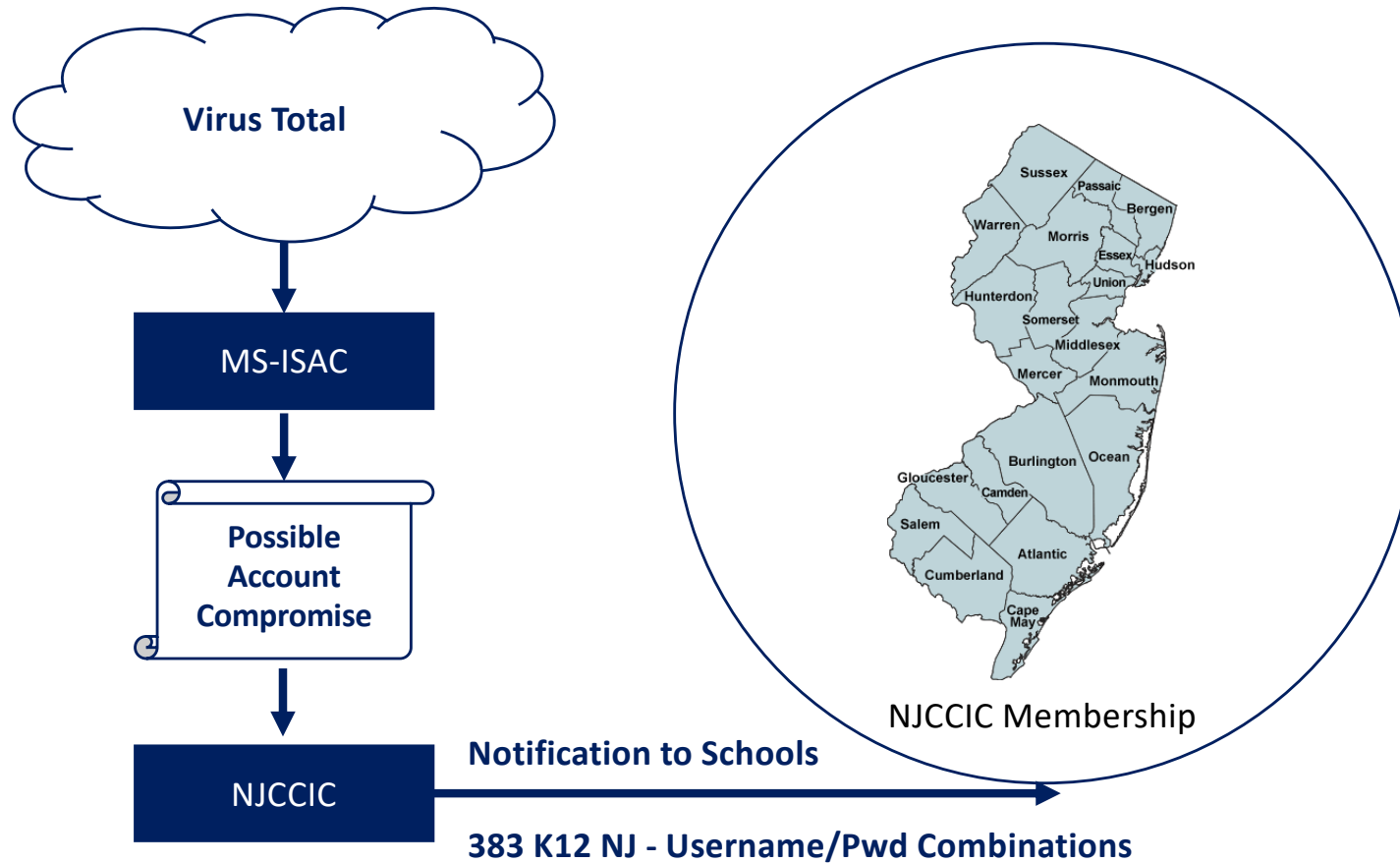


Public – Private Partnerships



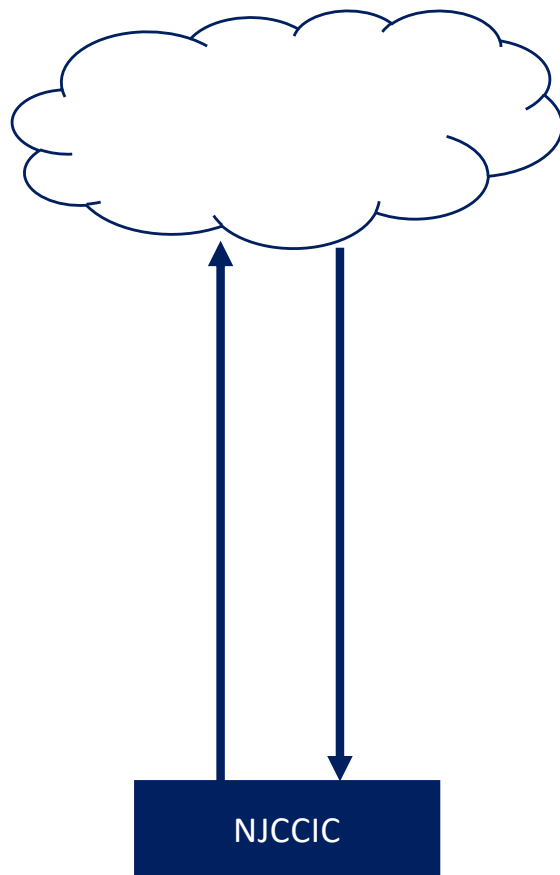


Public – Private Partnerships





Credential Compromise



1.4 Billion Username/Pwd
Combinations

Email Address: Password

Source – Multiple: Compiled
from numerous data
breaches over the past
several year

Ransomware



NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

August 22, 2019

TLP: WHITE

An Enduring Threat Greatly Impacting Public and Private Sector Organizations

Ransomware: *A type of malware that attempts to extort money from victims by restricting access to a computer system or files. This is accomplished by encrypting files that can only be decrypted with a key held by the malicious actor.*

In this week's bulletin, we are focusing on the growing number of ransomware attacks that are impacting public and private sector organizations nationwide, crippling operations, and resulting in devastating financial losses. Despite all the warnings and awareness campaigns that prescribe risk mitigation strategies and tactics to help ward off ransomware attacks, they continue to be a highly successful and profitable endeavor for those actors who carry them out. On August 16th, 22 public sector organizations in Texas fell victim to a [coordinated ransomware attack](#). One week later, their recovery efforts continue with major systems still offline. In July, Louisiana Governor Edwards declared a [State of Emergency](#) to deal with a spate of ransomware attacks. The [Georgia Department of Public Safety](#) was also victimized along with a growing list of victim organizations nationwide. Closer to home, the [Stevens Institute of Technology](#) was hit by ransomware on August 8th and their IT team is racing to restore their systems in time for the start of the fall semester.



Ransomware Risk Mitigation Strategies

TLP: WHITE



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

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

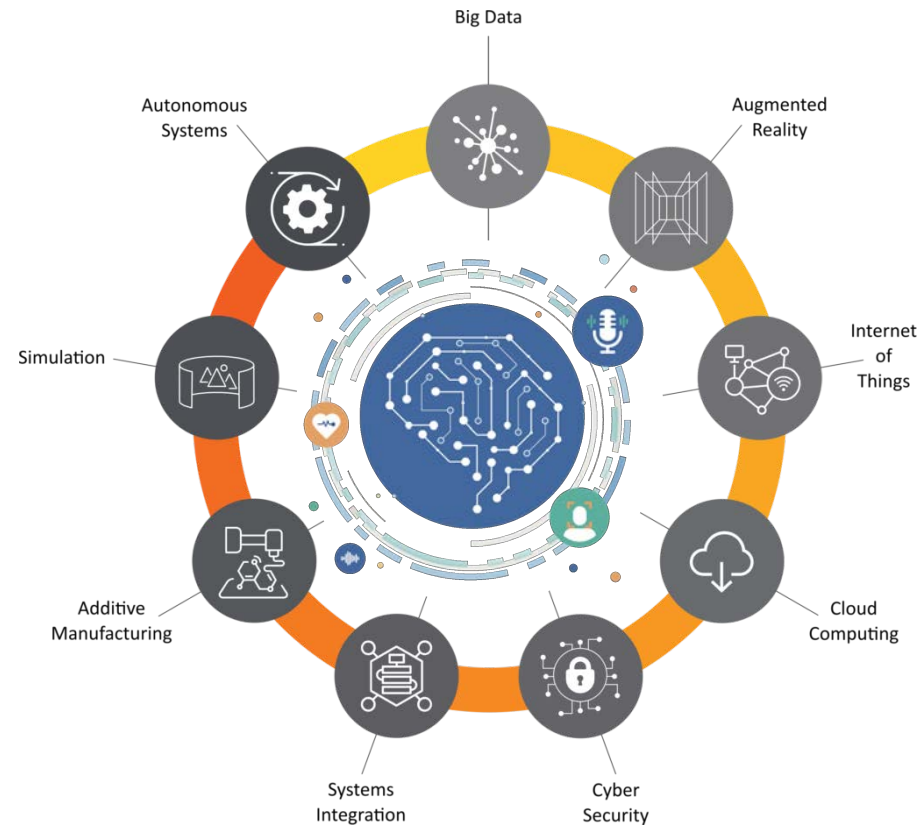
- Ensure anti-virus software is up-to-date with the latest definitions and schedule scans as often as permitted.
- Enable automated patching for operating systems, software, plugins, and web browsers.
- Follow the [Principle of Least Privilege](#) for all user accounts and enable User Access Control (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.

www.cyber.nj.gov/threat-profiles/ransomware

Cybersecurity in the 4th Industrial Revolution



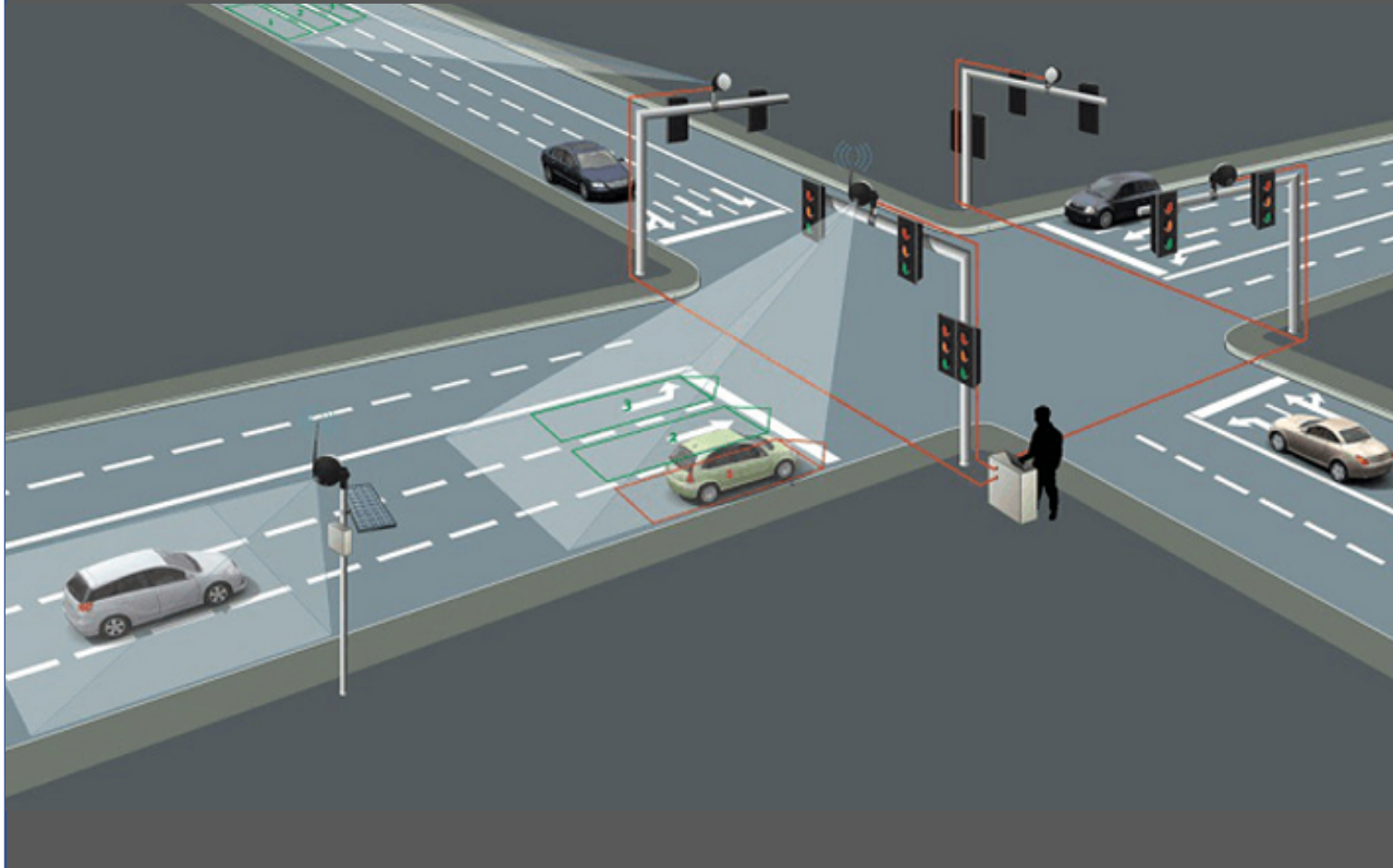
The 4th Industrial Revolution

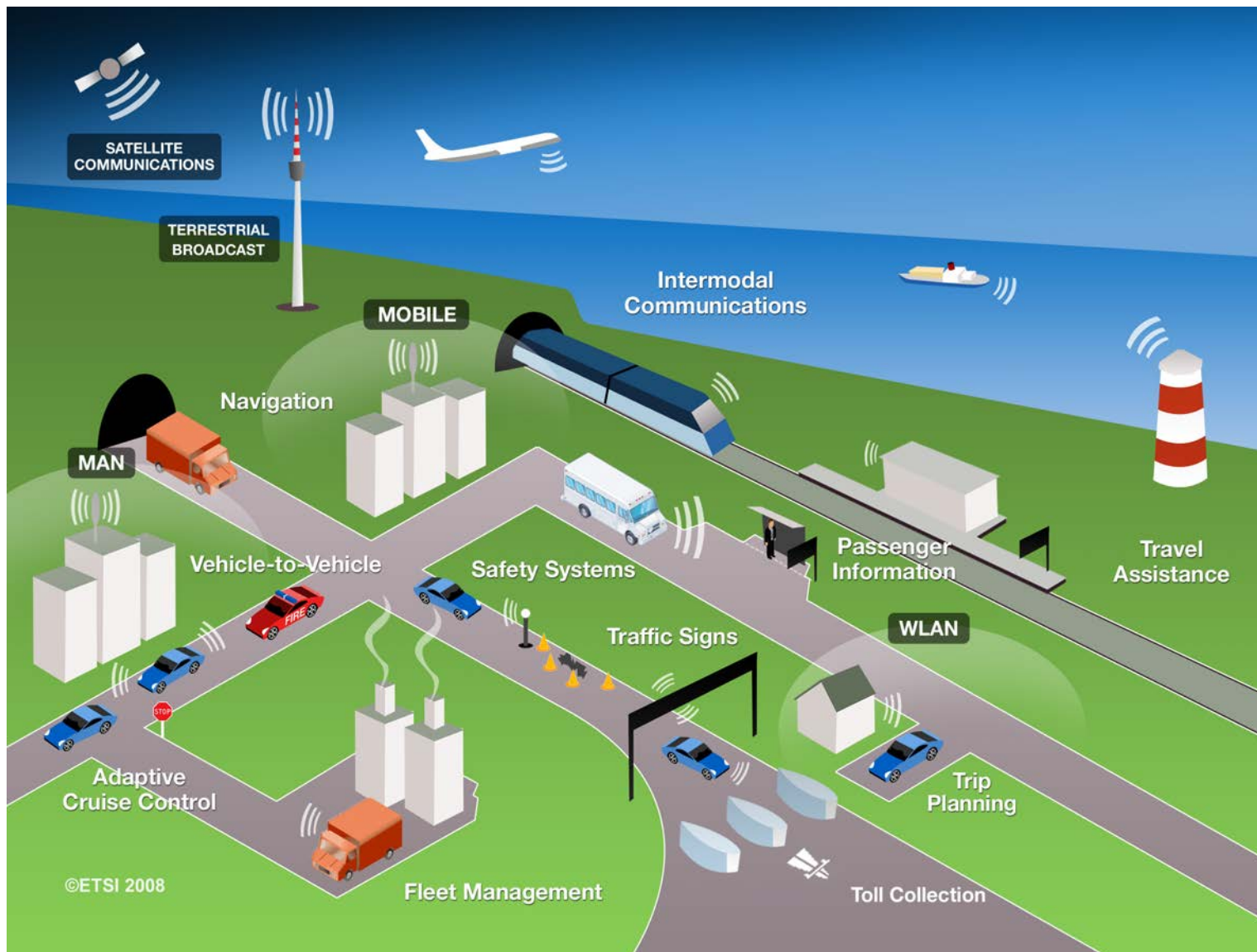


Cyber-Physical Convergence

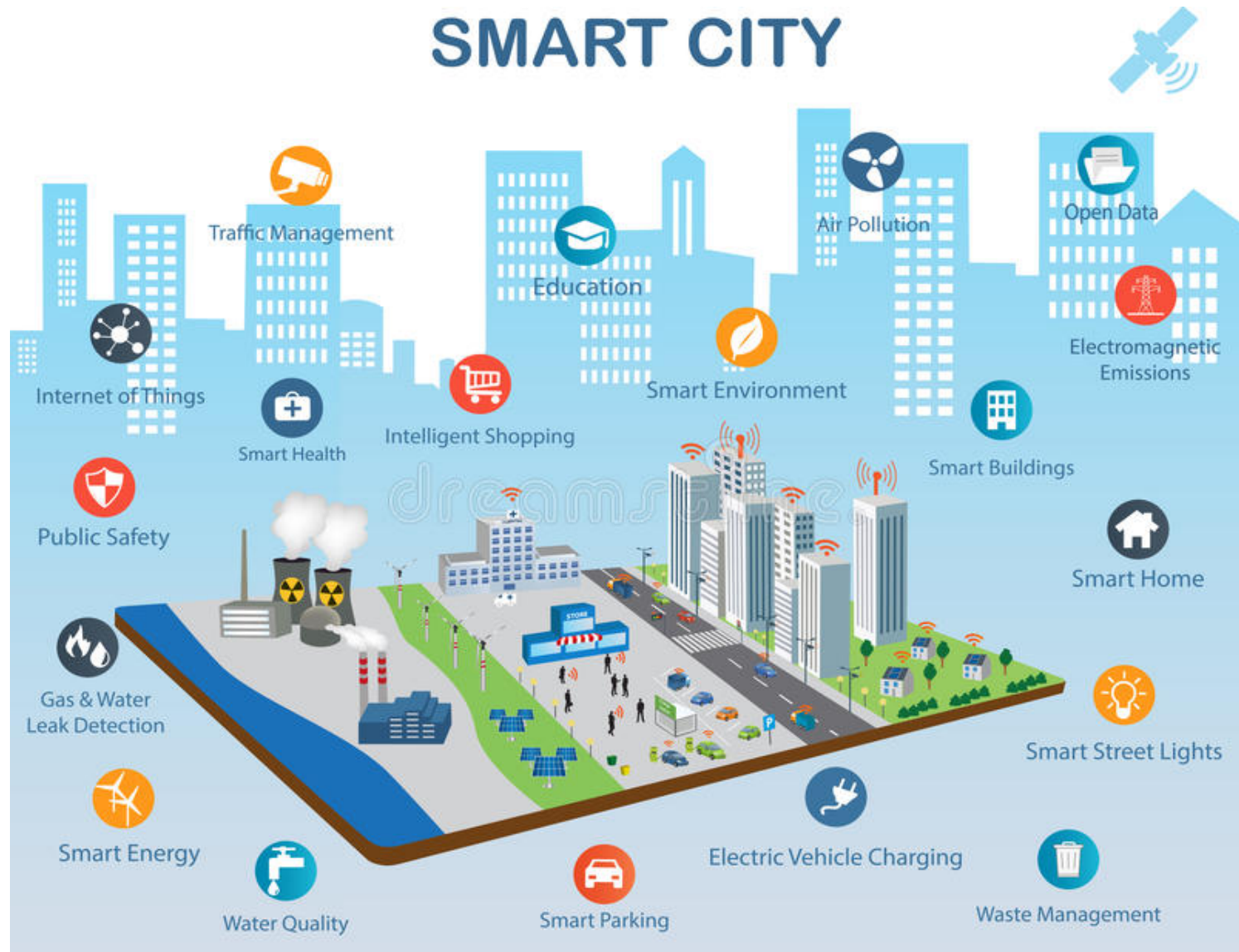


Intelligent Traffic Systems





SMART CITY



Achieving Digital Resilience



Cybersecurity Program Components

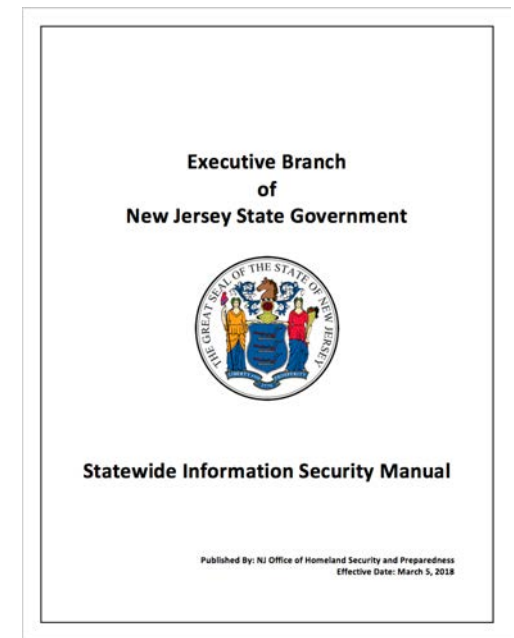
DETECT	Threat Management Continuous Monitoring; Security Operations; Penetration Testing.	RESPOND	Incident Management & Forensics Respond and Investigate Incidents.	RECOVER	Continuity of Operations & Disaster Recovery Backup/Recovery; Fail Over; Restore.
PROTECT	Data Protection Data at Rest and In Transit; Networks, Systems, Applications.	Identity & Access Management Ensure Only Authorized Users Have Access to Resources; Privileged Identity Management.		Vulnerability Management Identify and Remediate Weaknesses in Systems and Applications.	
IDENTIFY	Risk Management Identify and Protect Most Critical Systems; Third Party Management.	Compliance Management Demonstrate Fulfillment of Statutory, Regulatory, and Contractual Obligations.		Security Architecture Configuration Management; Security and Privacy by Design.	
CHANGE	Governance Alignment of Security Program with Business Objectives, Program Management, Policies/Standards, Finance, Metrics.				
	Culture and Change Execution Tone from the Top; Champion and Sustain Change Across Organization; Talent Management; Security Awareness.				



Statewide Information Security Manual

Intended to assist organizations in applying 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.

- Derived from Industry Standards: NIST CSF, NIST 800-53, CIS Top 20 Controls, etc.
- 37 Control Areas
- Applicable to all information assets owned, leased, licensed, managed, or used by Executive Branch agencies
- Published: March 2018















Statewide Information Security Manual Control Areas

- Program Management
- Organizational Security
- Compliance
- Personnel Security
- Security Awareness and Training
- Rules of Behavior
- Risk Management
- Privacy
- Information Asset Management
- Security Categorization
- Media Protection
- Cryptographic Protection
- Access Management
- Identity and Authentication
- Remote Access
- Security Engineering and Architecture
- Configuration Management
- Endpoint Security
- Embedded Systems
- Mobile Device Management
- Network Security
- Cloud Security
- Change Management
- Information Asset Maintenance
- Threat Management
- Vulnerability and Patch Management
- Continuous Monitoring
- Security in Software Development
- Security for Publicly Accessible Websites and Services
- Project and Resource Management
- Capacity and Performance Planning
- Third Party Management
- Security Assessment and Authorization
- Exception Management
- Physical and Environmental Security
- Contingency Planning
- Incident Response



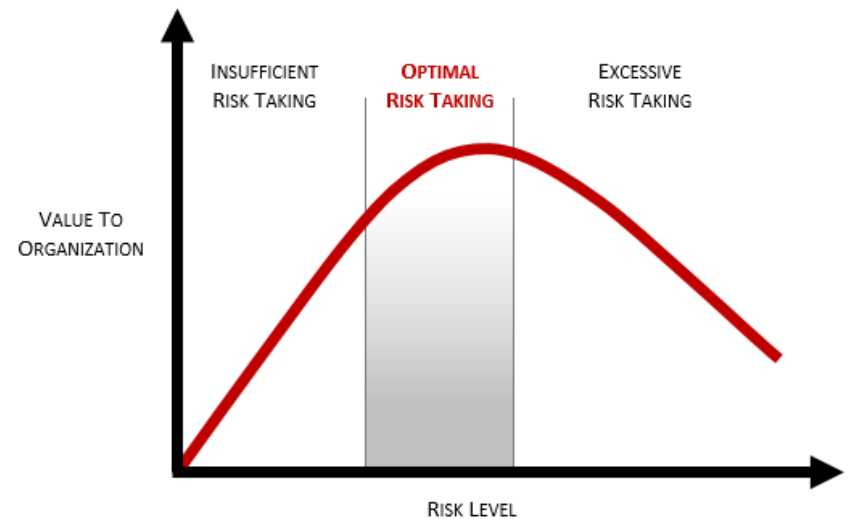
NJCCIC Cybersecurity Program Controls Assessment

1.0 - INFORMATION SECURITY PROGRAM MANAGEMENT (PM)						
The organization establishes and maintains a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.						
PM	Control Objectives	Implementation				
		Not Implemented (0%)	Minimally Implemented (1-33%)	Partially Implemented (34-66%)	Mostly Implemented (67-99%)	Fully Implemented (100%)
1.1	Roles and Responsibilities: The organization establishes a management structure and responsibility for information security, and appoints an individual assigned with the mission and resources to centrally manage coordinate, develop, implement, and maintain an organization-wide security program.					
1.2	Information Security Policies and Standards: The organization develops, implements, and governs processes and documentation to facilitate the implementation of organization-wide information security policies and associated standards, controls, and procedures.					



Achieving Digital Resilience

- All Threats/ All Hazards
- Collaborate or Perish – One Team/One Fight
- Prioritize information assets based on risks
- Security and Privacy by Design
- Develop Culture of Cybersecurity
- Test continuously to improve incident response





NJCCIC Services

Weekly Bulletin

Presentations and Training

Threat analysis

Threat profiles

Be Sure to Secure

Cyber Risk Self-Assessment

Incident Reporting/Response



Connect with the NJCCIC



NJCCIC@cyber.nj.gov



www.cyber.nj.gov



1-833-4-NJCCIC



[@njcybersecurity](https://twitter.com/njcybersecurity)