RHODE ISLAND STATE CYBERSECURITY STRATEGY

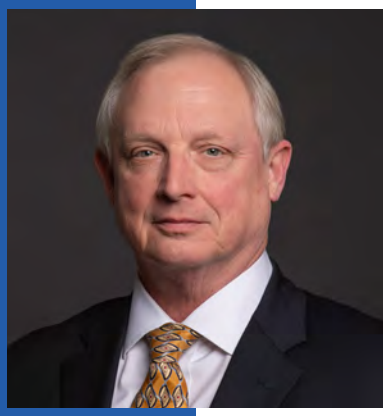



A MESSAGE FROM THE GOVERNOR

Four years ago, I created Rhode Island's first Cybersecurity Commission, which remains just one of a handful of its kind in the country. The Commission was tasked with creating a clear strategy to protect Rhode Island from cyber threats while growing our state's industry and economy. The 2019 Rhode Island State Cybersecurity Strategy is an extension of that important work. Our modern infrastructure is more than just roads and bridges; it's also the digital connections we're making faster and more frequently than ever before. In the ever-changing technology ecosystem, it is imperative that Rhode Island stays up to speed by focusing on the people, processes, and technology fueling industry expansion. Statewide, over 13,000 people currently work in jobs in or related to cybersecurity.

Our state is now uniquely positioned to improve its security while supporting our growing economy and innovation ecosystem. I look forward to working across the public and private sectors to refine and expand Rhode Island's cybersecurity strategy, statewide, and prepare our citizens for the technological challenges of the 21st century.

Gina Raimondo
Governor
State of Rhode Island and Providence Plantations



A MESSAGE FROM THE STATE CYBERSECURITY OFFICER

The Rhode Island Cybersecurity Strategy aims to prepare Rhode Island's public and private sectors for the digital challenges of the 21st century by increasing the security and resilience of our state's digital systems and private sector critical infrastructure. By doing so, we will improve the state's cyber hygiene, increase the resiliency of systems both public and private while maturing the ecosystem underpinning technological innovation. Acting on and implementing the state cybersecurity vision, goals and objectives, will enhance and add resilience to the growing economy, increasing the security of future government operations, the resilience of our critical infrastructure, and bolster the security and privacy of the individual citizen.

The Rhode Island Cybersecurity Strategy follows on the heels of the important work accomplished by the 2015 Rhode Island Cybersecurity Commission. The recommendations published by the Commission have served as the state's strategic roadmap since October of 2015. Upon my arrival, I implemented the Commission's recommendations which have already served to limit the business and economic impacts of sophisticated malware and persistent phishing attacks targeting our state.

I am indebted to the Governor and her staff, the leadership and members of the 2015 Rhode Island Cybersecurity Commission, and the Governor's Homeland Security Advisory Board, for their support, review, and input to this strategy. Without the cooperation and teamwork of the Rhode Island National Guard cyber forces and the Rhode Island State Police cyber leadership, with the Department of Administration's Enterprise and Technology Services and Strategy Department, we would not have the cybersecurity response capacity we now enjoy. Finally, without close collaboration with the State CIO/CDO and the State CISO, publishing a credible and executable Cybersecurity Strategy for the state would not have been possible.

Mike Steinmetz
Rhode Island State Cybersecurity Officer

STRATEGIC OVERVIEW

Page 6: Rationale for a Strategy and Approach to Cybersecurity

The Strategy opens with the importance of cybersecurity to the citizens of Rhode Island, detailing the rationale for publishing a State Cybersecurity Strategy. The Strategy's vision and three primary goals provide the reader with a framework for the risk-based approach that the state will use to improve security and fuel innovation.

Page 10: Cybersecurity Threats and Risks to Rhode Island

The evolving threat to Rhode Island grows every day; from those who wish to compromise and steal data, to those who deny citizens the use of digital systems, such as the internet. Here, the reader will learn about the threats and risks to the state's critical infrastructure, democratic processes, government services and individual citizens.

Page 16: Approach to Countering the Threats

Rhode Island will mitigate the cyber threat by systematically reducing the likelihood and impact of an attack. State employees and citizens have an important role to reduce harm and increase digital resiliency. This section concludes with a paragraph on leadership. Leadership plays an important role in cultural change. Strong leadership will make the state more digitally secure and resilient.

Page 18: Strategic Goals and Actions

The Rhode Island Cybersecurity Strategy sets expectations for improvement. This section opens by restating the three strategic goals that provide the framework for the State's Cybersecurity Strategy. Each goal pairs with its beneficial outcome. The remaining pages lay out a series of objectives and actions grouped under each goal, along with an estimated time frame for completion. A top-level matrix of the state's strategic goals and objectives is aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Page 28: Appendices

The Strategy closes with four appendixes that provide the reader with a glossary of cybersecurity-related terms, a listing of state organizations with a cyber mission, a list of best practices for every Rhode Island citizen and resources for additional cybersecurity information.

WHY HAVE A STATE CYBERSECURITY STRATEGY?

The citizens of Rhode Island depend on a complex system of globally connected devices for the delivery of goods and services and for overall economic prosperity. So many of our activities, whether at work or in our personal lives, are now enabled by computers or mobile devices. Each of us counts on these devices—and the complex, interconnected digital system supporting them—to deliver our services, communicate with loved ones, conduct business, operate machinery, and store sensitive information. Often, threats to these complex systems have dominated headlines and our personal discussions, because we depend on the systems to enable safe elections, reliable social services, energy for our homes, telephone communications, and secure business transactions. Indeed, we expect that the computers we use, and the digital systems within which they operate, will protect our personal data, securely transmit our business transactions, protect our critical infrastructure, and provide a secure means by which the state economy can grow.

Developing and publishing a strategy sets Rhode Island on a positive course for improved cybersecurity resilience. The Rhode Island Cybersecurity Strategy does this by establishing a clear vision then laying out objectives and stating expected outcomes. Taking the actions enumerated in the Strategy will provide the state with ways to measure progress. At the same time, every objective and action listed should have a life that evolves with our changing environment. The Cybersecurity Strategy lays out the first round of objectives and actions, intended to inspire and invite dialogue about future cybersecurity objectives for the state.

VISION STATEMENT

Make Rhode Island safe, robust and resilient by building a culture of innovation and growth that delivers the security needed to live, work and govern in the 21st century.

STRATEGIC GOALS

1. Increase the resilience of the infrastructure supporting the health, safety, and security of citizens, the government and the state's economy. Prepare Rhode Island's public and private sector infrastructure for the digital challenges and opportunities of the 21st century.
2. Create a digitally aware culture by improving cyber awareness within the state.
3. Mature the ecosystem underpinning technological innovation within the state. Growth of the state's innovation ecosystem will enhance and strengthen the growing economy, the security of future government operations, the resilience of our critical infrastructure, and the security and privacy of the individual.

The Rhode Island Cybersecurity Strategy provides an effective means of implementing Governor Raimondo's vision for a cyber-secure Rhode Island. In 2015, the Governor created the Rhode Island Cybersecurity Commission, whose 27 members identified opportunities to increase the state's digital security and resilience. In May 2017, the Governor created the Rhode Island Homeland Security Advisory Board by Executive Order, which concluded the work of the Cybersecurity Commission and began an effort to address state digital resilience holistically. The appointment of a State Cybersecurity Officer brought attention to this important topic. The Cybersecurity Strategy serves as the next important step in realizing the vision and strategic goals first laid out by the Governor and the 2015 Commission. The Cybersecurity Strategy builds on the 2015 Commission's considerable accomplishments to set out a well-defined set of objectives for the next five years.

The Strategy adheres to cybersecurity best practices established by the National Institute of Standards and Technology (NIST), the International Standardization Organization (ISO), the Office of Management and Budget, [Office of Management and Budget, Federal Cybersecurity Risk Determination Report and Action Plan, May 2018] and others. The Strategy's objectives establish a solid foundation for cybersecurity governance within the state. They also lay out a proactive approach to growing our innovation ecosystem, designed to develop the advanced technological capabilities needed by the state in the years to come. This focus on an innovation culture, and the ecosystem underpinning innovation, is unique among state strategies. Only through investment in innovation and translational research will we build the base of diverse advanced technology and the skilled workforce required to meet tomorrow's challenges. Focusing on the research ecosystem and skilled labor will help grow our labor and technology base at a sufficient rate to counter growing threats to our digital systems and our citizens.

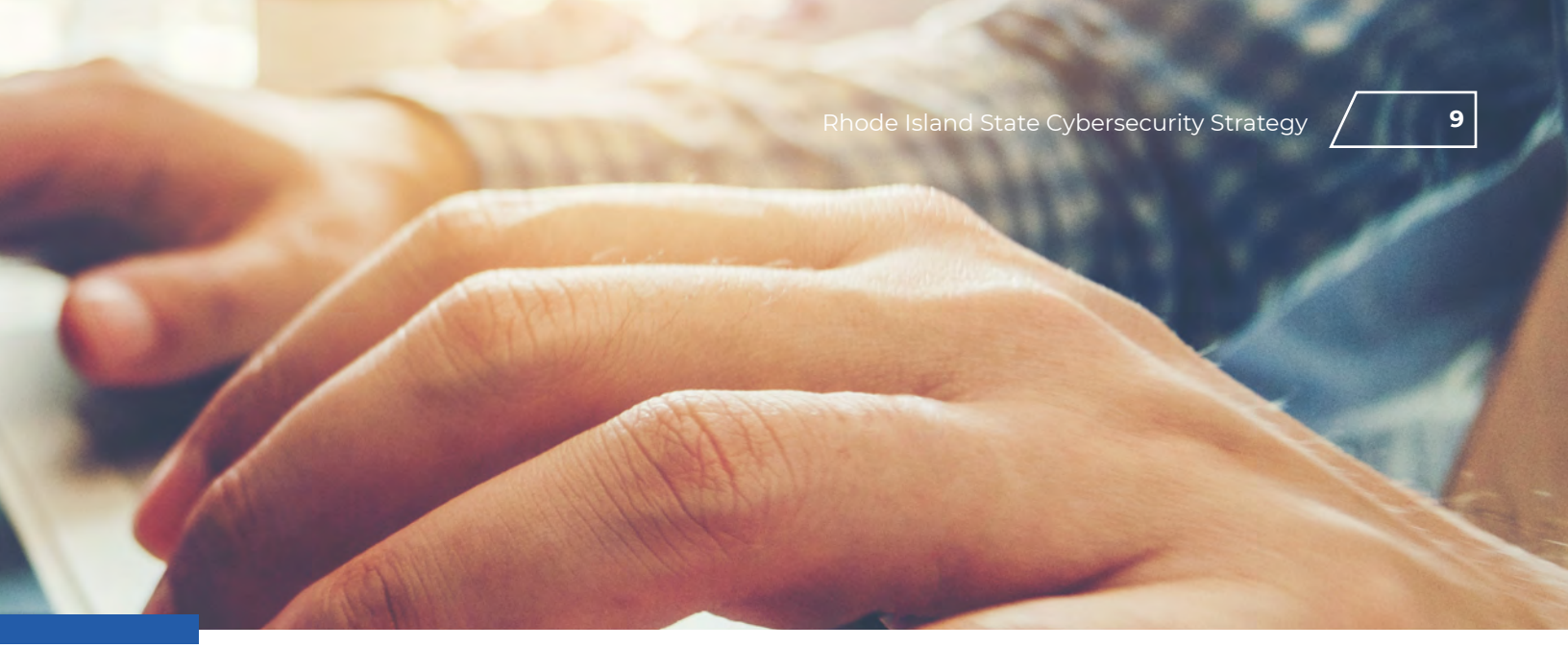
The year-long development of the Cybersecurity Strategy included an analysis of the 2015 Commission's findings, internal and external audits, and a review of third-party assessments. Together, these provided a substantive background on the current state of cybersecurity and greatly assisted in identifying our state goals. The Strategy's vision, objectives and actions were drafted and then reviewed by the Governor's Homeland Security Advisory Board. They were then further refined by the state's Cybersecurity Officer, Chief Information Officer, and Chief Information Security Officer, greatly assisted by Commerce Corporation cyber leadership, State Police Computer Crimes leadership and National Guard cyber professionals, so that objectives would match desired end states and outcomes.

BUILDING A RISK-BASED APPROACH

Rhode Island will employ a risk-based approach to cybersecurity, based on the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF) and risk methodology. Identifying systemic risks that may affect secure delivery of essential services, is of the highest priority. Assessment of the State's cybersecurity risk will help leadership prioritize risks in a manner relevant to Rhode Island's current technology and processes. Once risks are identified and prioritized, the state can execute cost-effective remediation. The state can also reduce systemic risks by effectively integrating risk-management practices, human-focused cyber hygiene, and secure engineering solutions delivered in a seamless and transparent process. This risk-based approach also prepares the state for greater collaboration with, and support from, the U.S. Department of Homeland Security National Risk Management Center.

IMPORTANCE OF PRIVATE SECTOR-PUBLIC SECTOR INFORMATION-SHARING

Public-private partnership is key to a cyber-resilient Rhode Island. The private sector drives nearly all growth in technology and cybersecurity. Greater collaboration with the private sector will result in more effective information-sharing, ensure greater trust, and enhance the resilience of critical infrastructure. There are federal, regional and state-level venues for information-sharing and collaboration. With continuous emphasis on improving trust, collaboration will evolve and enhance the state's ability to respond to and recover from cybersecurity breaches. Due to the global nature of cyber threats, close relationships with regional and federal agencies with cybersecurity missions or equities will increase the state's overall situational awareness. State organizations that create cybersecurity resilience are realized through partnerships created by the Joint Cyber Task Force, formerly the Cyber Disruption Team, and other organizations. The Joint Cyber Task Force (JCTF), led by the Rhode Island State Police, has evolved, moving beyond cyber disruption towards a more holistic approach that empowers and leverages strong public-private partnerships. Nurturing such partnerships at all levels will provide Rhode Island with an opportunity for continued growth and resilience, building the capacity needed to respond to major cyber incidents. State investments, such as the JCTF, align with other federal efforts within the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and others to bring higher levels of trust and resilience to the state, the region, and our nation.



INTELLIGENCE-LED ANALYTICS

Our ability to see threats, and to better understand them, enables defenders to make proactive decisions and then act appropriately on them. To employ an intelligence-led approach, we must better use the state's Fusion Center, capitalize on the Fusion Center's relationships with the private sector, integrate with other Fusion Centers and federal entities, and balance the crosscutting equities of other relevant actors. An intelligence-led approach will allow Rhode Island to limit its focus to the state, its processes, and its culture, enhancing the efficiency of our investments and security operations.

STRATEGIC ROADMAPS

To counter and stay ahead of ever-growing cyber threats, the state must have a strategic roadmap that integrates the various human and technology elements impacting our cybersecurity. A technology roadmap will provide a more complete view of technology investments that improve cybersecurity and provide optimal value for taxpayers' money. When there are difficult fiscal decisions to make, the state will need to have clear priorities readily at hand. Using a risk-based approach is the most successful way to address competing priorities. This approach clarifies the business impacts of security solutions and assigns them a risk-based priority. Using this approach in the strategic technology roadmap will help guide leadership discussions around challenging fiscal decisions.

THE EVOLVING THREAT

Understanding digital threats reduces fear, uncertainty and doubt. Threats are evolving in maturity and sophistication, as is the size of the target we must protect. The volume, variety and speed of cyber threats increase every hour of every day. It is important to determine what opportunities cyber attackers have to compromise confidentiality, integrity, availability, and veracity of data and critical systems.

Cybersecurity professionals create cyber intelligence by combining this knowledge with an understanding of attackers' capabilities and intent. This process paints a better picture of the evolving threat and how it might impact important systems and data, and it informs our risk-management practice to better align limited resources.

China and "probably one or two other" countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber-attack, the head of the National Security Agency told a Congressional panel...

Admiral Mike Rogers, Director, National Security Agency (NSA) November 2014

THE EXTERNAL THREAT

External cyber threats can be described three ways: by what the threat actor's capabilities are, what the actor's intentions are, and what opportunities the threat actor has to attack. On one side of the scale, you have thieves who are trying to monetize information they steal or deface digital property. Given the right sources of intelligence and data, the feedback loop (i.e., intelligence-led discovery) can be relatively fast with this threat. More advanced, and therefore elusive, are activists and some nation-state threats. These are hackers or hacking organizations trying to make a political or sociological point. It can take up to a year to locate or identify the activity of these attackers. Most difficult are high-end spies and sophisticated saboteurs. These attackers employ state-of-the-art stealth tactics to avoid being found and are often supported directly or indirectly by nation-states.

THE INTERNAL THREAT

Internal threats can be broadly grouped into threats from (1) people, (2) processes and (3) technology. (1) The people in question are state employees or third-party vendors. We can divide people-based threats into human error and malicious insider threats. In the first case, the employee or vendor does not understand that their actions may inflict harm by exposing sensitive data or compromising processes. The risk from employee human error can be greatly reduced through a robust and continuous cybersecurity awareness training program that delivers year-round education in social engineering and phishing tests. The risk from third-party vendors can be reduced by clear contract terms requiring adherence to nationally recognized security standards, security audits, and continuous monitoring.
In the case of malicious insider threats, the employee or vendor understands the harm they can inflict and knowingly exposes sensitive data or compromises processes. Risks from malicious insiders can be reduced by employing various technological and behavior-based solutions. (2) Then there are internal threats due to processes. These issues indicate that internal security controls are inadequate or aren't being followed properly. Risk-based governance reviews can identify corrective actions to remediate process-related threats. (3) Finally, internal threats from technology usually stem from technology debt, which means technology so old it can't be protected in today's digital environment or technology whose manufacturer no longer supports it with security updates. Technology debt can introduce severe vulnerabilities inside systems. Systems with technology debt should be identified for replacement or outsourced as managed services, in which case the security risk is transferred from the state to a managed service vendor.

RISKS TO THE STATE'S CRITICAL INFRASTRUCTURE

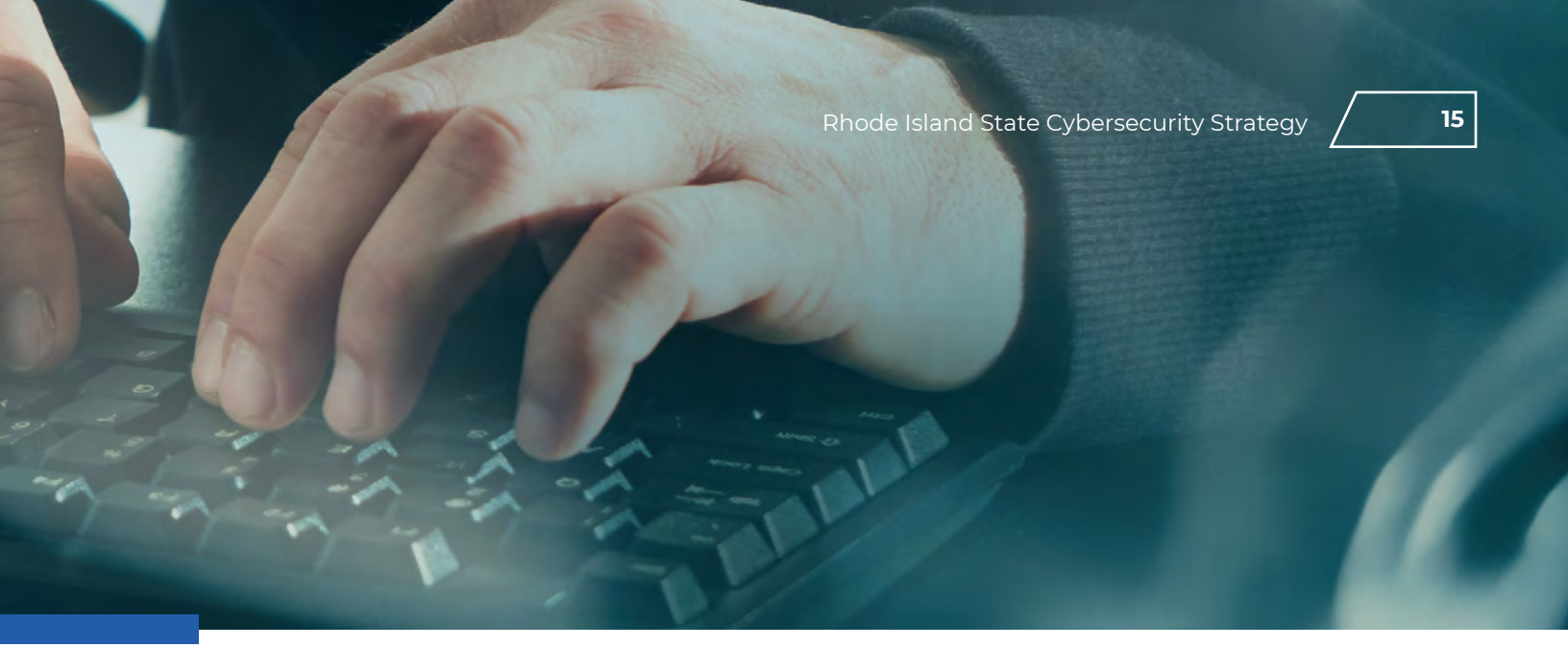
In 2014, the Director of the National Security Agency spoke with unaccustomed public candor about threats to our critical infrastructure that U.S. intelligence agencies have identified [https://www.c-span.org/video/?322853-1/hearing-cybersecurity-threats]. Since that time, Ukrainian electrical substation power systems have been downed twice by attackers armed with offensive cyber weapons. Malware has been identified within U.S. power company systems but has, to date, been successfully neutralized. Other risks to U.S. critical infrastructure have been noted in the press, regarding communications router malware and the digital security of our financial systems. Information-sharing and advisory councils led by the U.S. Department of Homeland Security (DHS) address most of these areas. Addressing the threat at the national level is important. Our vigilance at the state and regional level is of equal importance and serves to support our public-private partnerships, which enable information-sharing to help increase our state's resilience and ability to respond to attacks. We must learn more about our systems in order to know where risk resides. Intrusion and attacks are inevitable, so we must learn to operate our critical infrastructure with that expectation. To this end, we must identify and protect the essential elements of our critical infrastructure, be ready to defend those elements when under attack, and prepare to respond and recover quickly. Close public-private partnership is essential to quick response and recovery.

RISKS TO DEMOCRATIC PROCESSES

The newest area, identified as critical infrastructure by the DHS, is our election systems. We must deploy and defend our election systems—and the people, processes, and technology underpinning them—in a fashion that assumes they will always be targets for foreign influence and manipulation. Taking this approach will improve our systems' resilience, reducing the uncertainty and doubt foreign entities wish to implant. The 2018 midterms highlighted not only the technical intrusions from foreign nations into election systems in other states, but also the widespread use of manipulated news and information. We must address voters' privacy and secure the process and technology by which they exercise their right to vote. We must also address the manipulative foreign influence that spreads disinformation and lies disguised as fact; citizens need avenues to check facts quickly and easily. Citizens must be able to feel secure that the information they draw on is accurate, that voter registration locations protect their privacy, and that the machines and processes handling their votes are both resilient and redundant. No process will ever eliminate all threats or ensure 100-percent security, but undertaking an intelligence-led, risk-based approach will significantly increase the resiliency of our democratic systems and reduce voter uncertainty.

RISK TO GOVERNMENT SERVICES

Rhode Island's government services are at risk every day. State employees are the first line of defense, safeguarding citizens' personally identifiable information and other confidential data and processes, such as tax data and vehicle licensing portals. They do their part by taking cyber awareness training and following written policy about using state systems. If data were exposed or processes compromised, attackers could steal data to sell or hold it for ransom. Compromised systems could also interrupt, slow or stop the flow of essential services to citizens. All types of threats (internal or external, willful or inadvertent) can expose confidential data or compromise the confidentiality, integrity, and availability of state services. While we can't entirely eliminate the risk, we can greatly reduce the likelihood of a successful attack, through thoughtful actions by trained "cyber-aware" employees and prudent implementation of security policy, processes, and controls. Similarly, employing clear policy, processes and training increases our resilience, allowing government services to quickly recover if attacked. Implementing the state's strategic goal number two will deliver increased resilience, preparing Rhode Island's public and private sectors for the digital challenges of the 21st century.



RISK TO CITIZENS

Our citizens face many risks to their personal information, their secure online transactions, their sensitive data, and more. Identity theft is at an all-time high, due to the number and size of global data breaches, as are malware infections that can, for example, activate a device's camera without the user knowing. Malware can also take the form of ransomware, disabling access to a citizen's computer. Digitally enabled products should undergo security-related scrutiny, including household items like digital thermostats, smart devices like Alexa or Google Assistant, and Wi-Fi-enabled products like baby monitors. Citizens' mobile devices are not immune and can also be infected by viruses. Some applications by default provide location and other private data when users fail to change the manufacturer's factory defaults. Moreover, user habits can figure prominently in personal risk, when citizens over-share details on social media or intentionally breach system safeguards in order to load untested applications onto their devices. Many of the hazards can be reduced significantly by employing best practices for personal and online safety. See Appendix C for a list of best practices for all Rhode Island Citizens.

COUNTERING THE THREAT: HOW DIGITAL SECURITY IS EVOLVING

Defending against the evolving cyber threat has changed from the reactive defense-of-the-perimeter ("moat and castle") approach employed in the early 2000s. Today, finding and removing threats requires more sophisticated approaches, such as a layered defense integrated with continuous monitoring and remediation. Additionally, threat hunting and advanced analytics are employed to locate latent threats and remediate effects before they have a chance to cause harm.

and vendors will build a near real-time picture of the threats to, and health of, our digital systems. These professionals and vendors must employ best practices in security operations, governance risk & compliance, vendor management, and secure architecture. Finally, timely development, dissemination, and revision of enterprise information technology and cybersecurity policies—coupled with coordinated assist visits, assessments and audits—provide a final layer of assurance and defense.

Evolution Of Cybersecurity

Nascent	Reactive	Proactive	Predictive	Next Generation
• 8/5 monitoring • Long review-based analysis • Irregular Patching • Limited GRC • Isolated Remediation • Point Solutions	• Assume an attack will occur & treat the symptom • Static signature analysis (looking for bad things dormant on the system) • Port blocking • Domain name system logging & analysis	• Prevent & contain attacks • Eliminate intruder advance • Detect adversary activity on endpoints • Hunt for indicators of adversary activity in the network	• Anticipate & react in real-time • Automated malware analysis • Real-time (+encrypted) traffic inspection & classification based on app, user, & content • Automated cyber security incident response	• Continuous Monitoring • Continuous Diagnostics and Remediation (CDR) • Next Generation Firewalls (NGF) • Continuous Threat Hunting • Advanced Intelligence Analytics • Integrated with other security disciplines (Physical, Personnel, etc.) "Concentric Ring Defense"
Typical 2004	State of the Art 2006	Best practice since ~2011	Industry leading ~2014	Future State Of Security in RI 2018 >

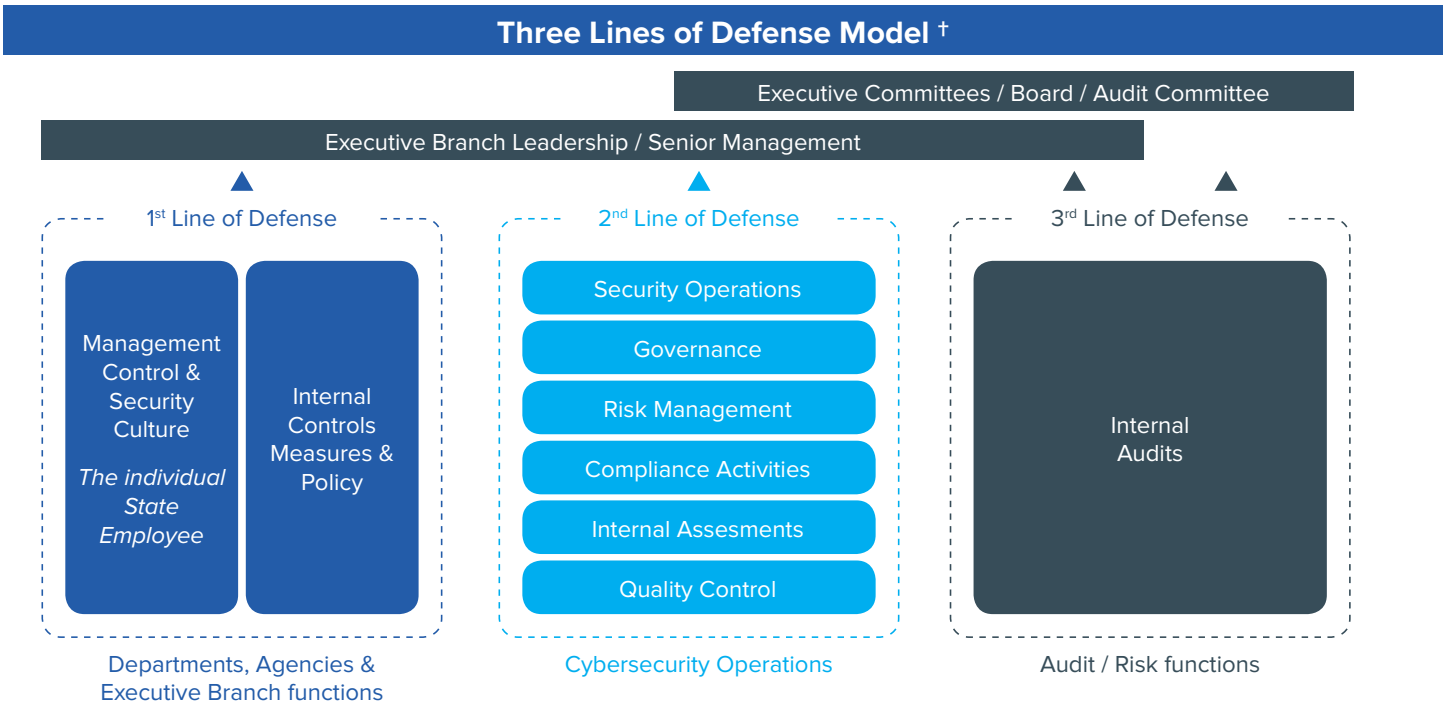
State of Rhode Island is moving quickly to a proactive and predictive approach. Next-Gen is aspirational for 2022

The sophistication of today's threat also requires a multidisciplinary approach to defense and resiliency. People, process, and technology all need to be harmonized and working together to counter intrusions and the inevitable presence of threats within our systems. Cyber hygiene within the state is of the highest importance, and each state employee plays an important role in the security of the state's systems and data. We must improve our cyber hygiene by training every state employee in basic cybersecurity threats and best practices. We can never completely eliminate human error, however, so it is equally important that we give attention to process and technology. Along with cybersecurity awareness training, the state is investing in cybersecurity professionals and vendors who will collaborate to provide relevant information and intelligence. An approach integrating cybersecurity professionals

Together, all these factors provide what is known as the "Three Lines of Defense" approach.

Let's look more closely at these three "lines." The first line of defense is the security culture and the individual state employee. Management controls, internal controls, and state policy must clearly articulate this responsibility and accountability for departments, agencies, and executive branch functions. The second line of defense is comprised of Enterprise Technology Services and Strategy (ETSS) intelligence, information, and security monitoring operations, coupled closely with governance risk and compliance activities. The third and final line is internal audit functions and risk analysis and risk governance functions, along with occasional external audits and necessary regulatory functions.

Adopting a complete lifecycle approach to cybersecurity helps protect the state from sophisticated modern cyber attackers. Over a period of years, the state's Department of Information Technology has evolved, adding or reorganizing agencies, departments and organizations. To keep pace with the increasing risk of cyber attack, the Rhode Island Cybersecurity Strategy focuses on culture and training (cyber hygiene), combining resources and expertise to protect data and systems. Siloed approaches to cybersecurity can place state systems at risk, due to inconsistent or sometimes nonexistent controls. Once implemented, the Rhode Island Cybersecurity Strategy will begin to improve resilience through broad lifecycle approach to security.



RESOURCE & REVIEW COORDINATION

The strategy will be reviewed annually. Departments and agencies will use the objectives, actions and illustrative time frames, to build their own action and resource plans within the normal state budgetary cycle.

The Department of Information Technology will schedule strategy reviews and resource coordination meetings, ensuring that the approach to both is as integrated and efficient as practicable.

LEADERSHIP

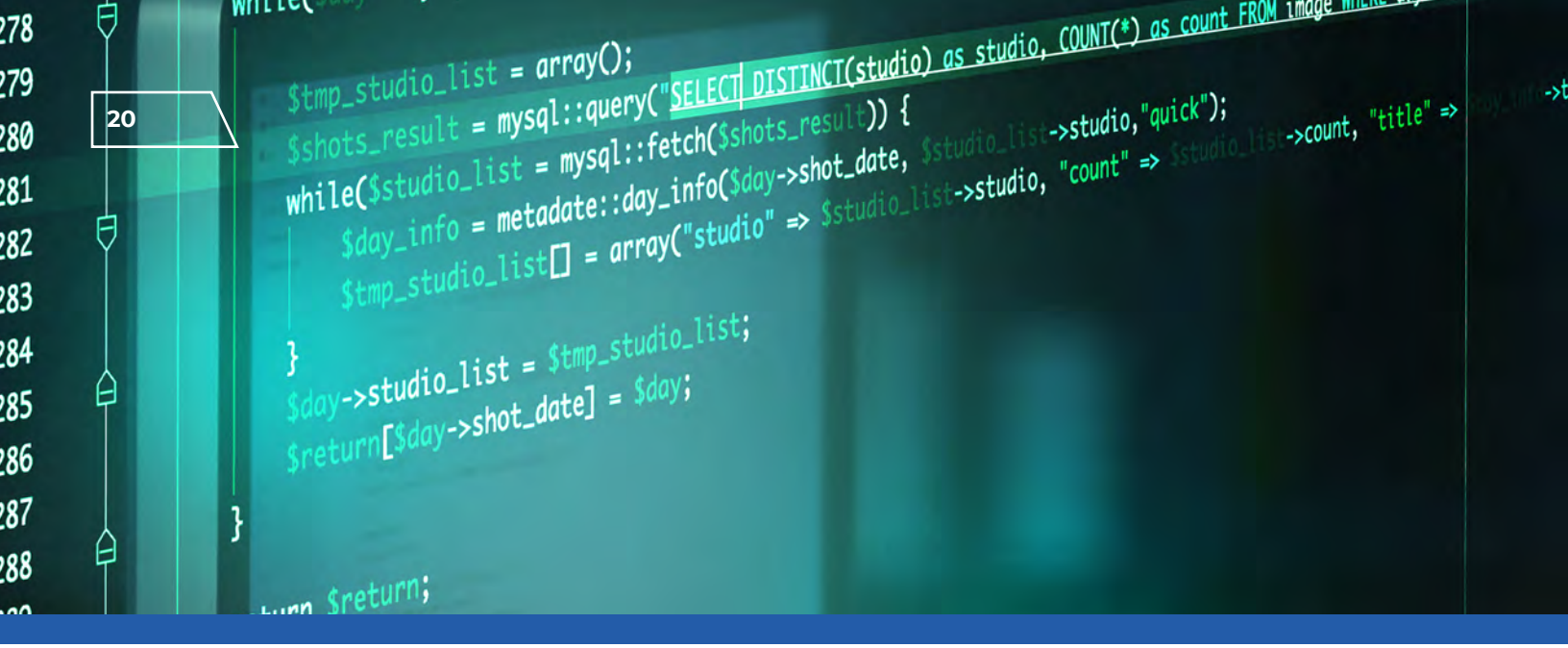
The Rhode Island Cybersecurity Strategy identifies opportunities for state leadership to assume greater responsibility and accountability for the digital resilience of state organizations. The Strategy will not work without a shared vision that puts accountability for digital security on all of our shoulders. Rhode Island state employees must lead by example. They must understand that the good work they do, and essential services they provide to citizens, rely largely on the security of our systems, which depends in turn on each employee's commitment to staying knowledgeable about, accountable for and engaged in cybersecurity.

† Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, Article 41

STRATEGIC GOALS AND EXPECTED OUTCOMES

Goal	Expected Outcomes
STRATEGIC GOAL NUMBER 1 Increase the resilience of the infrastructure supporting the health, safety, and security of citizens, the government and the state's economy. Prepare Rhode Island's public and private sector infrastructure for the digital challenges and opportunities of the 21st century.	• An effective, risk-based, and intelligence-led approach that measures cybersecurity maturity is in place, supporting business impact and security-related decisions having to do with people, process, and technology. • The state technology roadmap provides leadership with the information needed to make decisions, set priorities, and employ quantifiable metrics to measure improvement. • The State of Rhode Island DoIT leaders employ and report metrics that confirm that state systems are protected to the highest levels of confidentiality, integrity, and availability. Rhode Island citizens, other states, and federal agencies have confidence in Rhode Island's digital resiliency and the confidentiality, integrity, and availability of essential data and systems. • Post-exercise lessons learned (about the state's critical infrastructure preparedness) identify areas for improvement that are acted upon and tracked, improving the resiliency of the critical infrastructure. • The state measures and reports on the level of awareness about risks to state systems, processes, and sensitive data, and observes a decrease in the time required to recover from security incidents. • Increased trust between the private and public sector, regarding information-sharing, results in greater shared threat awareness between the sectors. • National Guard cyber response capacity is optimized and institutionalized and, when exercised or tested, demonstrates improved response and reduced recovery time after incidents. • State of Rhode Island citizens have access to and utilize cybersecurity information that improves their personal security and privacy.

Goal	Expected Outcomes
STRATEGIC GOAL NUMBER 2 Create a digitally aware culture by improving cyber awareness within the state.	• Continuous cybersecurity training metrics track improved cyber hygiene in state government. • Effective behavior-based policies for cybersecurity are in place and have a positive effect on the security of state operations, systems, and data. • Annual threat assessments demonstrate continuous improvement in the cyber hygiene of state government. • Information and intelligence-sharing improve the security posture of the state. • State democratic processes and the governance of those processes are more secure. • Citizens have access to needed information and confidence in its accuracy and truthfulness. • Citizens' cybersecurity awareness improves with access to best practices that help them protect personally identifiable information and improve the security of their online operations.
STRATEGIC GOAL NUMBER 3 Mature the ecosystem and promote a culture of technological innovation within the state.	• Academic institutions develop more public-private innovation partnering opportunities. • Academic institutions increase the amount of translational research in cybersecurity, artificial intelligence, and quantum computing. • Growth of high-technology startups spinning off from translational research doubles in 5 years. • An academic consortium that shares technology and intellectual property provides greater opportunity for academic collaboration and private-sector investment. • Rhode Island hosts an annual technology fair for small and medium-sized businesses involved in cybersecurity and advanced technology. • An established, international cybersecurity-related event is held annually in Rhode Island. • Venture capitalists establish offices within Rhode Island, funding cybersecurity and advanced technology startups. • Space within the Providence Innovation Campus is at maximum capacity in 2 years. • Innovation campuses at URI and other locations are 70 percent pre-leased before completion.

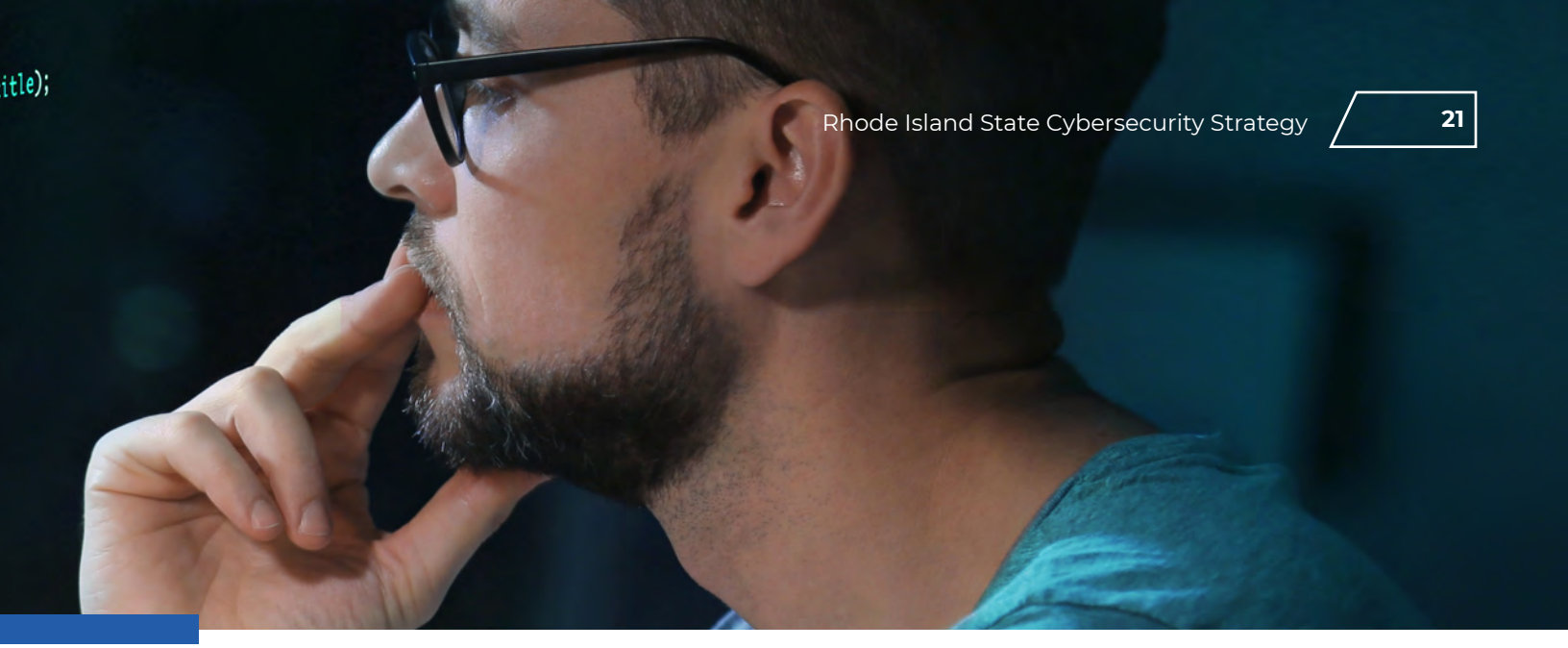


OBJECTIVES AND ACTIONS FOR GOAL NUMBER 1
STRATEGIC GOAL NUMBER 1

Increase the resilience of the infrastructure supporting the health, safety, and security of citizens, the government and the state's economy. Prepare Rhode Island's public and private sector infrastructure for the digital challenges and opportunities of the 21st century. Time Frame ~1-3+ years.

Strategic goal number one addresses the evolving threat to the public sector, to private sector critical infrastructure, and to private citizens' systems and devices. Because of the complexity of the systems and the increasing complexity of threats, we can assume there will be times when the confidentiality, integrity, or availability of processes, systems, and data are compromised. Goal number one acknowledges this inevitability and addresses the need to build in resilience, so as to minimize the time needed to respond and recover from cyber-attacks.

Objective	Action
Objective 1.1: Implement a risk-management program for cybersecurity. (2 years)	Develop a governance program for risk-based methodology. Adopt and institutionalize the cybersecurity risk program.
Objective 1.2: Establish an intelligence-led cybersecurity program within state government that reduces cyber-attack response time and optimizes vulnerability management. (1 year)	Source appropriate intelligence material, germane to state architectures and processes, as well as vetting procedures for the security operations team.
Objective 1.3: Modernize state government information and security technology. (2 years)	Develop an enterprise technology roadmap that modernizes the enterprise architecture and technology. Develop a prioritized inventory of critical and high-value cyber assets. Establish and employ a third-party vendor for security-related best practices. Incorporate modernization of security operations and technology in the state technology roadmap.
Objective 1.4: Exercise new technology and security enhancements annually. (3 year test plan)	Develop an annual test and exercise plan for enterprise security technology.



Objective	Action
Objective 1.5: Mature state government security processes. (2 years)	Form an action team, led by CIO and CISO, to review statewide processes and recommend changes.
Objective 1.6: Develop a cyber talent plan for the state. (More than 3 years)	Partner with State Human Resources and use third-party assessment data, plus department and agency feedback, to build a cybersecurity talent plan with career progression options.
Objective 1.7: Exercise with critical infrastructure representatives, where exercise objectives identify resiliency-related improvements to counter the cyber threat. (3 years)	Develop or modify objectives of existing exercise plans with critical infrastructure where exercise outputs identify resiliency-related improvements to state systems.
Objective 1.8: Streamline the State Police Joint Cyber Task Force's role in responding to state-level cyber incidents and grow its capacity. (2 years)	Form a team of the JCTF and other state and non-state entities to build options that grow JCTF and Fusion Center cyber information-sharing and cyber analytics capabilities.
Objective 1.9: Mature the incident response processes between primary incident responders, the Rhode Island Emergency Management Agency, and other public and private resources. (1 year)	Finalize the RIEMA MCIRP with the U.S. DHS representative for cybersecurity region one. Then finalize with state stakeholders and exercise plan annually.
Objective 1.10: Publish monthly metrics that indicate the level of awareness about cyber threats and the time required to recover from cybersecurity incidents. (1 year)	Develop a dashboard for monthly use that tracks changes in threat awareness and recovery time.
Objective 1.11: Evaluate and implement improvements to public-private information-sharing. (2 years)	Engage with Joint Cyber Task Force, FBI InfraGard, and other organizations to improve interactions between public and private entities, for better information-sharing.
Objective 1.12: Determine National Guard response capacity, and institutionalize integrated response into all state government cyber incident response plans. (2 years)	Engage with National Guard cyber forces and develop a National Guard cyber response capacity plan. Institutionalize Guard agreements with the State of Rhode Island, via a memorandum of understanding or memorandum of agreement.

OBJECTIVES AND ACTIONS FOR GOAL NUMBER 2
STRATEGIC GOAL NUMBER 2

Create a digitally aware culture by improving cyber awareness within the state. Time Frame ~1-3+ years.

Goal number two addresses the relationship between humans and technology. Policy must support the security of the state enterprise and must work efficiently with the humans operating and interfacing with the technology. The people involved must understand their role and the range of possible outcomes from their actions. Collectively, the people, process and technology combine to create the digital culture. When they employ best practices, it improves the cyber hygiene for all.

Objective	Action
Objective 2.1: Create a security culture within the executive branch and other state agencies. (1 year)	Form a cybersecurity policy working group. Develop policies, procedures, and guidelines that set standards for cyber hygiene within the Executive Branch. Conduct an annual cyber threat assessment. Expand the state cybersecurity awareness training program, making it available to Treasury, the Courts, and the Secretary of State, as licensing permits.
Objective 2.2: Ensure examples of best practices from other states are incorporated into Rhode Island cybersecurity policies. (2 years)	Use the cybersecurity policy working group to review best practices of other states. Develop a method to measure policy outcomes and report quarterly or semiannually to the state policy working group.
Objective 2.3: Use a threat-assessment dashboard and metrics to measure improvement, and review them monthly. (1 year)	Develop threat metrics that measure cybersecurity hygiene in the Executive Branch. Develop a threat dashboard that displays cyber hygiene trends for the executive.
Objective 2.4: Enhance security information-sharing for state government and government/ quasi-government agencies. (3 years)	Create a community of interest among public CISOs and CIOs.

Objective	Action
Objective 2.5: Enhance security information-sharing between the public and private sectors. (3 years)	Create a community of interest among private critical infrastructure CISOs and CIOs. Support continued development of the Joint Cyber Task Force in shared public-private information-sharing.
Objective 2.6: Enhance security of democratic systems. (1 year)	Provide cybersecurity support to elections-related systems. Support state and academic efforts to counter cyber threats to state elections, state judiciary and other governmental processes.
Objective 2.7: Enhance Rhode Island citizens' cybersecurity awareness. (3 years)	Provide citizens with access to cybersecurity resources. Provide cybersecurity information and resources to Rhode Island businesses, growing capacity beyond that covered by the JCTF. Create internally and externally facing state cybersecurity webpages containing information resources for citizens. Support other government initiatives that provide cybersecurity awareness training to municipalities. Work with RIEMA to request more funding and assets to support cyber training within the state. Support public school initiatives that raise cyber awareness.
Objective 2.8: Enhance Rhode Island major cyber incident response capacity. (3 years)	Department of IT, RI National Guard, and RI State Police; Work with RIEMA to identify additional funding, training, and resources to build response capacity to a major cyber incident.

OBJECTIVES AND ACTIONS FOR GOAL NUMBER 3
STRATEGIC GOAL NUMBER 3

Mature the ecosystem and promote a culture of technological innovation within the state.
Time Frame ~2-4+ years.

Goal number three addresses key elements of the state's innovation ecosystem. Without technological innovation, cyber threats evolve while our ability to counter them recedes. A strong innovation ecosystem relies on robust translational research from leading universities and labs. The ecosystem then feeds startups with compelling and competitive business cases, creating jobs in advanced technology that in turn grow the economy. Underpinning the innovation ecosystem are events that provide technological exposition for investors and other business opportunities.

Objective	Action
Objective 3.1: Create environments for academic and public-private sector innovation. (2-3 years)	Create a Center of Excellence within the state with cyber as a key element. Build upon the partnerships with premier accelerators within the Rhode Island Innovation Hub, to grow innovation density in the state. Drive innovation-related activities into the innovation districts throughout Rhode Island.
Objective 3.2: Create an academic consortium committed to innovation. (2 years)	Extend existing innovation investments within Rhode Island academia with Wexford, Cambridge Innovation Center (CIC), and venture/private equity. Meet quarterly, driving innovation dialogues into the CIC Venture Cafe, focusing on venture capitalists' exposure to the evolving translational research in Rhode Island.
Objective 3.3: Create a consortium and a charter setting out the processes for academic sharing of technology and Intellectual Property. (2 years)	Charter an academic consortium of Rhode Island higher education institutions to share technology and intellectual property. Link existing work regarding Rhode Island innovation ecosystems with investments that benefit all of advanced technology. Bring more partnership opportunities, with national labs and others, into the innovation ecosystem.
Objective 3.4: Provide opportunities for the exposition of new technologies. (2-3 years)	Work with the Rhode Island Commerce Corporation to explore and evaluate regional and national opportunities for Rhode Island small and medium-sized businesses to demonstrate and display their technology and services.
Objective 3.5: Create thought leadership events that highlight Rhode Island cyber talent and innovation. (2-3 years)	Pull international events of note into Rhode Island. Create a unique event in Rhode Island that is of global importance.
Objective 3.6: Evolve the innovation ecosystem in Rhode Island. (3-4 years)	Leverage the work undertaken and produced by other working groups addressing gaps in the innovation ecosystem.


DISTRICT HALL

ALIGNMENT WITH THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK

Alignment of the Rhode Island Cybersecurity Strategy with the NIST Cybersecurity Framework	Identify	Protect	Defend	Respond	Recover
Strategic Goal #1 Increase the resilience of the infrastructure supporting the health, safety, and security of citizens, the government and the state's economy. Prepare R.I.'s public and private sector infrastructure for the digital changes and opportunities of the 21st century.					
Objective 1.1: Implement a risk-management program for cybersecurity.	•	•	•	•	•
Objective 1.2: Establish an intelligence-led cybersecurity program within state government that reduces cyber-attack response time and optimizes vulnerability management.	•				•
Objective 1.3: Modernize state government information and security technology.	•	•	•	•	•
Objective 1.4: Exercise new technology and security enhancements annually.	•				
Objective 1.5: Mature state government security processes.				•	•
Objective 1.6: Develop a cyber talent plan for the state.				•	
Objective 1.7: Exercise with critical infrastructure representatives, where exercise objectives identify resiliency-related improvements to counter the cyber threat.				•	•
Objective 1.8: Streamline the State Police Joint Cyber Task Force's role in responding to state-level cyber incidents and grow its capacity.				•	•
Objective 1.9: Mature the incident response processes between primary incident responders, the Rhode Island Emergency Management Agency, and other public and private resources.				•	•
Objective 1.10: Publish monthly metrics that indicate the level of awareness about cyber threats and the time required to recover from cybersecurity incidents.	•	•			
Objective 1.11: Evaluate and implement improvements to public-private information-sharing.	•			•	•
Objective 1.12: Determine National Guard response capacity, and institutionalize integrated response into all state government cyber incident response plans.				•	•

Alignment of the Rhode Island Cybersecurity Strategy with the NIST Cybersecurity Framework	Identify	Protect	Defend	Respond	Recover
Strategic Goal #2 Create a digitally aware culture by improving cyber awareness within the state.					
Objective 2.1: Create a security culture within the executive branch and other state agencies.		●	●	●	
Objective 2.2: Ensure examples of best practices from other states are incorporated into Rhode Island cybersecurity policies.		●			
Objective 2.3: Use a threat-assessment dashboard and metrics to measure improvement, and review them monthly.	●	●			
Objective 2.4: Enhance security information-sharing for state government and government/quasi-government agencies.	●	●			
Objective 2.5: Enhance security information-sharing between the public and private sectors.	●	●			
Objective 2.6: Enhance security of democratic systems.		●	●	●	●
Objective 2.7: Enhance Rhode Island citizens' cybersecurity awareness.		●	●	●	●
Objective 2.8: Enhance Rhode Island major cyber incident response capacity.				●	●
Strategic Goal #3 Mature the ecosystem and promote a culture of technological innovation within the state.					
Objective 3.1: Create environments for academic and public-private sector innovation.		●		●	●
Objective 3.2: Create an academic consortium committed to innovation.		●		●	●
Objective 3.3: Create a consortium and a charter setting out the processes for academic sharing of technology and intellectual property.		●		●	
Objective 3.4: Provide opportunities for the exposition of new technologies.	●	●			
Objective 3.5: Create thought leadership events that highlight Rhode Island cyber talent and innovation.	●				
Objective 3.6: Evolve the innovation ecosystem in Rhode Island.	●	●	●	●	●

APPENDIX A
GLOSSARY AND DEFINITIONS

CCU – Computer Crimes Unit
CDO – Chief Digital Officer
CIKR – Critical Infrastructure Key Resources
CIN – Cyber Intelligence Network
CIO – Chief Information Officer
CISO – Chief Information Security Officer
COS – Cyberspace Operations Squadron
CTAA – Coordinate, Train, Advise and Assist
DCO – Defensive Cyber Operations
DHS – Within Rhode Island the State's Department of Human Services
DHS – At the Federal level, The Department of Homeland Security
DoIT – Rhode Island Division of Information Technology
DoD – Department of Defense
DPS – Department of Public Safety
EO – Executive Order
ESF – Emergency Support Function
ESF-2 – Emergency Support Function Two; Communications
FBI – Federal Bureau of Investigation
FEMA – Federal Emergency Management Agency
FTC – Federal Trade Commission
FISCAM – Federal Information Systems Controls Audit Manual
FOUO – For Official Use Only
GAO – Government Accountability Office
GDPR – General Data and Privacy Regulations
HIPAA –Health Insurance Portability and Accountability Act
HSAB – Homeland Security Advisory Board
ICAC – Internet Crimes Against Children
ICS – Industrial Control System
ISAC – Information Sharing and Analysis Center
ISAO – Information Sharing and Analysis Organization
ISO – International Standards Organization
ISO – Independent System Operator (e.g., New England ISO)
ICS-CERT – Industrial Control Systems–Cyber Emergency Response Team
IT – Information Technology
JCTF – Joint Cyber Task Force
MOA – Memorandum of Agreement
MS-ISAC – Multi-State Information Sharing and Analysis Center
NCCIC – National Cybersecurity and Communications Integration Center
NG – National Guard
NIST – National Institute of Standards & Technology
NIST-CSF – National Institute of Standards & Technology Cybersecurity Framework
NSA – National Security Agency
PCII – Protected Critical Infrastructure Information
PII – Personally Identifiable Information
RIANG – Rhode Island Air National Guard
RIARNG – Rhode Island Army National Guard
RIEMA – Rhode Island Emergency Management Agency
RIFC – Rhode Island Fusion Center
RING – Rhode Island National Guard
RISP – Rhode Island State Police
SAD – State Active Duty
SCHS – State Cybersecurity and Homeland Security
SEOC – State Emergency Operations Center
STEM – Science, Technology, Engineering and Math
T32 – US Code Title 32
TLP – Traffic Light Protocol
US-CERT – United States Computer Emergency Readiness Team
U.S. DHS – United States Department of Homeland Security

APPENDIX B
STATE GOVERNMENT ORGANIZATIONS WITH A CYBER MISSION

State government agencies possess different functional roles, responsibilities, authorities, and capabilities that are instrumental to cybersecurity incident response.

RHODE ISLAND DIVISION OF INFORMATION TECHNOLOGY

The Rhode Island Division of Information Technology (DoIT) has been established as the lead state IT agency within the Executive Branch, responsible for providing secure, innovative, and reliable IT services in the most responsive and operational manner. Under the direction of the Chief Information Officer (CIO)/Chief Digital Officer (CDO), DoIT will:

- Direct IT service functions within the state apparatus, including both physical locations and digital systems, to ensure that business needs are met;
- Establish, develop, implement, and improve information security systems and functions to promote more effective and efficient IT administration within the state;
- Oversee the implementation and approval of IT policies, standards, and guidelines;
- Manage the delivery of IT services administered and supported by the state government;
- Assist and train the state's executive management to understand, prioritize, and manage current and future security risks;
- Audit and control security policies and procedures to ensure state agencies carry out their appointed functions;
- Distribute information on emergency security alerts, Virus Watch, and cybercrime and terrorism; and
- Investigate reported or discovered enterprise security violations.

In addition to the responsibilities listed above, DoIT provides a single point of contact for all IT service requests via the DoIT Service Desk. Agencies that may have a potential cybersecurity issue should contact the Service Desk immediately. DoIT will have primary cyber incident response responsibility for state agencies, unless criminal activity is determined or suspected.

RHODE ISLAND EMERGENCY MANAGEMENT AGENCY

If/when a disaster (natural or man-made) breaches state cybersecurity, the Rhode Island Emergency Management Agency (RIEMA) performs an essential coordinating and communications role. RIEMA uses an all-hazards approach to preparedness, response, recovery, and mitigation—while providing technical assistance and support to local, regional, and state entities. Critical infrastructure protection is a continuous process, with many interdependencies that cross jurisdictions and natural boundaries. Protecting critical infrastructure is essential for resiliency in the state. RIEMA works proactively with key stakeholders to address persistent risks that threaten Rhode Island. As a member agency of the JCTF, RIEMA is responsible for:

- Organizing a scalable Cyber Section, with advice from the State Cybersecurity Officer, State CIO/CDO and JCTF Lead during a SEOC activation;
- Coordinating with specifically identified ESFs during a SEOC activation;
- Identifying CIKR within the state;
- Requesting the issuance of a State of Emergency Declaration through both the Governor's Office and FEMA;
- Assisting, as appropriate, in the restoration of communications and CIKR; and
- Coordinating federal support.

RHODE ISLAND STATE POLICE JOINT CYBER TASK FORCE (JCTF)

The Rhode Island State Police JCTF is the state's primary cybersecurity incident response team, when the capacity and capability of organic cybersecurity teams cannot defend, respond to, or recover from a cyber incident. The JCTF provides analysis and support before and during major cybersecurity incidents that affect critical infrastructure in Rhode Island and ensures continuity of services following an incident. As a communications conduit between federal, state, military, and private entities, the JCTF is comprised of members from the Rhode Island State Police CCU, RIFC, and individuals representing state government, information technology, academia, healthcare, finance, utilities, the private sector, and the defense industry. Bullet points below outline the membership of the JCTF.

Under the direction of the JCTF Lead, or Officer in Charge, the JCTF is responsible for:

- Acting as Incident Commander or other incident-specific authority during a SEOC Cyber Section activation;
- Performing primary interface or liaison duties for external communications and coordination for the JCTF;
- Overseeing the notification methods described in the State Communications Plan governing ESF-2: Communications;
- Managing the JCTF contact list;
- Organizing regular JCTF meetings with both core and associate members, as well as others;
- Investigating prosecutable criminal attacks during a cyber incident;
- Coordinating public and private-sector cybersecurity partnerships; and
- Coordinating cybersecurity end-user training and network security with municipal JCTF membership.

RHODE ISLAND STATE POLICE COMPUTER CRIMES UNIT

The Rhode Island State Police Computer Crimes Unit (CCU) is the lead agency for computer crimes investigations in Rhode Island. The CCU is primarily responsible for three operational areas: the Computer Forensic Laboratory, the Joint Cyber Task Force, and the Internet Crimes Against Children Task Force.

RHODE ISLAND FUSION CENTER

The Rhode Island Fusion Center (RIFC) is responsible for facilitating the efficient, timely, and accurate exchange of information between local, state, and federal agencies and private-sector organizations. Through a coordinated approach, the RIFC will augment law enforcement operations by acting as a centralized, comprehensive intelligence center to coordinate the exchange of threat intelligence on a statewide basis. The RIFC will collect, analyze, and disseminate threat intelligence to identify, investigate, and prevent malicious cybersecurity incidents and activities. Threat intelligence includes but is not limited to: threat levels, techniques adversaries employ, targeted systems and information, and any specific threat-related information that provides greater situational awareness to the JCTF membership, state government, and local government. Effective threat intelligence demonstrates the following characteristics:

- Accurate: Threat intelligence should be clear, concise, and complete. Inaccurate or incomplete information may prevent appropriate action or result in an improper response.
- Actionable: Threat intelligence should identify actions the recipient can take to counter the threat or provide sufficient information and context to allow the recipient to develop a suitable response.

- Relevant: Threat intelligence should have applicability within the recipient's operating environment, addressing what threats and adversaries the agency is likely to encounter. Recipients of threat intelligence should perform a vulnerability assessment to determine the degree of risk associated with a particular threat.
- Specific: Threat intelligence should describe the incident or adversary with a level of detail that successfully addresses the significance of the threat, to allow recipients to understand exactly how they will be affected by the threat.
- Timely: Threat intelligence should be delivered promptly, to provide sufficient opportunity for the recipient to anticipate the threat and prepare for a suitable response. The timeliness of threat intelligence is situational and depends on the consequences of the threat; the speed of attack; and the tactics, techniques, and procedures (TTPs) of the adversary.

During a cybersecurity incident, the RIFC is in a unique position to disseminate cybersecurity alerts among state agencies and the private sector, using the Homeland Security Information Network (HSIN), a secure and trusted national web-based portal for information-sharing and collaboration. The RIFC is responsible for coordinating threat intelligence and information-sharing to the Department of Homeland Security (DHS) and the FBI, as well as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Cyber Intelligence Network (CIN), an outreach network of corporate security, information security, and intelligence community professionals. Several state ISACs have been formed for industry sectors, including IT, communications, energy, and banking and finance. [See the National Council of ISACs website for a list of ISACs. Retrieved from http://www.nationalisacs.org]. As these information-sharing resources provide a platform for reporting threat intelligence, it is important to provide state agencies and the private sector with a clear, concise methodology for communicating levels of incident severity.

STATE CYBERSECURITY AND HOMELAND SECURITY

SCHS is responsible for driving all inter-agency processes related to cybersecurity. Leading SCHS, the State Cybersecurity Officer/Homeland Security Advisor (HSA) is a member of the Governor's cabinet and provides strategic advice to the Governor and fellow cabinet members on cybersecurity and homeland security matters. In addition, SCHS serves in a coordinating capacity by developing and maintaining a common homeland security operating picture between RING, JCTF, RIEMA and DoIT, as well as other state and federal agencies.

RHODE ISLAND NATIONAL GUARD

The Rhode Island National Guard (RING) plays a critical role in providing military support to civil authorities during local emergencies. The RING is an advanced cybersecurity resource for detecting, analyzing, researching, and responding to network intrusions and vulnerabilities. The Rhode Island Air National Guard's 102nd Cyberspace Operations Squadron (COS) and the Rhode Island Army National Guard's Defensive Cyber Operations (DCO) component house a significant number of airmen and soldiers with advanced cybersecurity skills and capabilities. These units collectively support intelligence cyber operations, risk analysis, network intrusion detection, network intrusion response, signature management, digital forensics, and ethical hacking. In addition, personnel from these units are core members of the JCTF. Operating out of Quonset Air National Guard Base in North Kingstown, Rhode Island, the RIANG 102nd COS is an Air Combat Command (ACC) unit that provides Cybersecurity Service Provider (CSSP) functionality. CSSP incorporates actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense (DOD) information systems and computer networks. Similarly, the RING's DCO, operating out of Camp Fogarty in East Greenwich, Rhode Island, offers operational tactics with authorized defensive actions against imminent threats, providing skilled and equipped mission-ready units in support of the National Military Strategy and the State, as required. The Rhode Island National Guard can operate under several authorities. At a time when the exact nature of the event has not yet been fully characterized and/or very short-term direct support is needed, the National Guard can (via direct request for support) respond to clearly defined supporting tasks, for up to 72 hours. This narrow and limited support mission is conducted under the authority granted to them by Defense Policy Memorandum 16-002 in a coordinate/train/advise and assist (CTAA) role. Extended support by the guard can be garnered under their State Active Duty authorities. Statewide emergencies or disasters may warrant activation of the National Guard under their U.S. Code Title 32 authorities. CTAA can be authorized by the Adjutant General. State Active Duty and Title 32 both require actions/activation by the Governor.

APPENDIX C

BASIC BEST PRACTICES FOR ALL RHODE ISLAND CITIZENS

CONSIDER TAKING THESE ACTIONS

1. Change your account passwords. Use a long pass-phrase that is easy for you to remember, rather than an 8-10-digit password that is difficult to remember. It is important not to use the same password for multiple accounts.
   * Consider getting a secure a password-keeper.
2. Patch your systems. If you are running Windows XP or 8, upgrade to Windows 10 or later. Set patches for OS to "auto update." This is applicable for Mac OS as well. Follow this step for your phones, tablets, etc.
3. Buy a clean, detachable external hard drive. Buy the detachable hard drive new from a reputable dealer.
   * DO NOT use an old hard drive, a hard drive somebody gave you, or a hard drive that you happened to find somewhere.
   * Back up your documents/files with your new detachable hard drive, then DISCONNECT it from your computer and keep it in a safe place.
4. Use two-factor authentication wherever possible. Yahoo and Google offer this option. Other applications may also offer two-factor authentication; call the vendor or organization and ask.
5. Encrypt your laptop hard drive and your new detachable hard drive that you just used to back up your documents /files.
6. Log on to social media platforms and check your privacy settings.
7. Subscribe to a Domain Name System (DNS) service. This will help you navigate the internet with enhanced safety.

BE SAFE ONLINE

1. Delete emails from people you don't know WITHOUT opening them.
2. Do not click on hyperlinks or open attachments in emails without confirming the identity of the sender. Same for texts on your cell phone.
3. Look at the address line (URL) of seemingly genuine emails from banks and other institutions. Do this by hovering over hyperlinks with your mouse. If the address looks suspicious, contact the sender via a publicly available number to confirm they sent you an email.

   * Microsoft will never phone you or send you an email telling you your system has been hacked.
4. Never give out your username and/or password over the phone.

   * Your bank or other legitimate institutions will never ask you for your online passwords or PIN codes.
5. Ensure you are in a secure online session when entering personal data online. You will know this by the addition of an "s" after "HTTP" and a lock symbol: Secure | https://. When you are finished, close your browser.
6. Limit what you share online. Something posted online will generally remain public forever.
7. Discuss online safety with children. Threats to children fall into 3 categories: strangers, friends and themselves.

   * Check out the Federal Bureau of Investigation's (FBI) website on safe online surfing tips for students and teachers: https://sos.fbi.gov/
8. Discuss online safety with those not "born digital," including senior citizens.
9. Own a small business?
   a. Check out the Federal Trade Commission's (FTC) website for small businesses: https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics
   b. Check out the U.S. Department of Homeland Security's (DHS) "Stop Think Connect" website: https://www.dhs.gov/stopthinkconnect
   c. Check out the FBI's website for cyber hygiene tips: https://www.fbi.gov/investigate/cyber#How-to-Protect-Your-Computer

APPENDIX D
LINKS TO OTHER CYBERSECURITY INFORMATION

CYBERSECURITY FOR SMALL BUSINESSES

https://www.globalcyberalliance.org (Small Business Toolkit, Quad 9 and DMARC for email)

https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics

FBI SAFE ONLINE SURFING (AGE-APPROPRIATE GAMES AND LEARNING)

https://sos.fbi.gov

THE FBI'S WEBSITE FOR CYBER HYGIENE TIPS

https://www.fbi.gov/investigate/cyber#How-to-Protect-Your-Computer

THE U.S. DEPARTMENT OF HOMELAND SECURITY'S (DHS) "STOP THINK CONNECT" WEBSITE

https://www.dhs.gov/stopthinkconnect

NOTES


RHODE ISLAND STATE POLICE
PUBLIC SAFETY COMPLEX