After Action Report / Improvement Plan November 2013

Rhode Island Corporate Community Cybersecurity Exercise (CCSE)

Conducted on October 9, 2013

CIAS CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY

SALVE REGINA UNIVERSITY PELL CENTER for INTERNATIONAL RELATIONS and PUBLIC POLICY

This page intentionally left blank.

HANDLING INSTRUCTIONS

1. The title of this document is: *Rhode Island Corporate Community Cybersecurity Exercise (CCSE) After Action Report / Improvement Plan*.

2. The information gathered in this report should be handled as sensitive information. This document should be safeguarded, handled, transmitted and stored appropriately.

3. Reproduction of this document, in whole or in part, without prior approval from one of the listed Points of Contact (POCs) below is prohibited.

4. At a minimum, the attached materials will be disseminated only on a need-to-know basis and when unattended, will be stored in a container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

5. Points of Contact:

Rhode Island Corporate Cybersecurity Initiative

Francesca Spidalieri
Initiative Lead and Cyber Leadership Fellow
Pell Center for International Relations and Public Policy
Young Building
518 Bellevue Avenue
Newport, RI 02840
(401) 341-2193
francesca.spidalieri@salve.edu

Exercise Director

G. Larry Thompson
Associate Director
Center for Infrastructure Assurance and Security
4350 Lockhill-Selma, Suite 100
San Antonio, TX 78249
(210) 458-2162
larry.thompson@utsa.edu

This page intentionally left blank.

CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY

Exercise Purpose and Design

The *Rhode Island Corporate Community Cybersecurity Exercise* was a tabletop exercise (TTX) conducted on Wednesday, October 9, 2013 at the Pell Center at Salve Regina University in Newport, RI. The purpose of the event was to work with organizational leadership to raise awareness and develop an understanding of cybersecurity issues and solutions.

Exercise Planning, Objectives and Resources

Planning and coordination began in August 2013. Two planning conferences were held in preparation for this exercise. The Initial Planning Conference was held on September 11, 2013 in Newport, RI. The planning team consisted of corporate community leadership. In this conference, the following concepts and objectives were established:

- Cybersecurity Awareness
- Policies and Procedures
- Training and Education
- Information Sharing and Analysis
- Business Continuity
- Resiliency Planning

The program has been made possible by funding from the Pell Center for International Relations and Public Policy at Salve Regina University.

Major Strengths

The major strengths identified in the exercise are:

- Rhode Island Corporate Community leadership recognizes the importance of cybersecurity and leadership's role in establishing and sustaining an organizational culture of cybersecurity.
- The Rhode Island Corporate Community has some informal information sharing relationships in place already.
- Strong relationships exist between organizations in the community, which is foundational to developing formal information sharing arrangements.
- Education of end users is a clear priority for participating organizations in the community.

Primary areas of improvement

The areas of improvement identified in the exercise are:

- Organizations should seize the emerging opportunities to identify new information sharing partners.
- Organizations that are currently sharing physical security information should expand their efforts to include cybersecurity information.
- Organizations should use their existing abilities, tools and relationships to develop methods and processes for sharing cybersecurity information.

Conclusion

This exercise provided organizational leadership the opportunity to come together to raise their awareness and develop an understanding of cybersecurity issues and solutions. It presented real-world issues and events to prompt participants to deal with incident response questions and to potentially share information with others. Leaders from the participating organizations were able to discuss cybersecurity and the impact it had on them during the entire exercise. Discussions centered on how to take further steps to better protect the organizations and Rhode Island's critical infrastructure.

SECTION 1: EXERCISE OVERVIEW

Exercise Details

Exercise Name
Rhode Island Corporate Community Cybersecurity Exercise (CCSE)

Type of Exercise
A cybersecurity awareness tabletop exercise (TTX)

Exercise Date / Duration
The exercise was conducted on October 9, 2013 and lasted six hours.

Location
The exercise was held at the Pell Center at Salve Regina University in Newport, RI.

Sponsor
The program was made possible by funding from the Pell Center for International Relations and Public Policy at Salve Regina University.

Guest Speakers
Dr. Jim Ludes, Executive Director, Pell Center for International Relations and Public Policy, welcomed participants to the exercise. He introduced Dr. Chris Demchak from the United States Naval War College who explained to participants the importance of resilience and operational gaming. Following her, Mr. Jim Lavoie, Chief Executive Officer, Rite Solutions, candidly discussed his organization's challenges with cybersecurity issues and the lessons they have learned. Finally, Rhode Island State Police Corporal John Alfred representing the Rhode Island Cyber Disruption team helped put the day's activities in perspective, briefing on the current threat and the importance of cybersecurity generally.

Scenario Type
Cyber intrusion and attack elements combined with supporting physical elements.

Exercise Planning Team

The following individuals attended the initial planning conference (IPC) on September 11, 2013:

Jason Black	Salve Regina University
Jeff Cares	Alidade Incorporated
Benjamin Lord	Bank of Newport
Colleen Medeiros	Bank of Newport
Chris Piacitelli	Citizens Bank
Francis Quigley	Pell Center, Salve Regina University
David Smith	Salve Regina University
Francesca Spidalieri	Pell Center, Salve Regina University

Participating Organizations

The following organizations participated in the October 9, 2013 exercise:

Alex and Ani, LLC
Alidade Incorporated
Beacon Mutual Insurance
Citizens Bank
Dell SecureWorks
Delta Dental
Dissect Cyber Incorporated
GTECH
Gurnet Consulting
IBM
MIKEL Incorporated
Oceanstate Financial Services
Pell Center for International Relations and Public Policy
Providence Water Supply Board
Purvis System Incorporated
Raytheon Company
RDW Group
Rite Solutions
Salve Regina University
Strategy and Management Services
Rhode Island Cyber Disruption Team
Rhode Island Small Business Development Center
Rhode Island State Police / Rhode Island State Fusion Center
U.S. Department of Homeland Security
U.S. Naval War College

Number of Participants and Support Staff

30 Participants
1 Moderators/Controllers
4 Facilitators

35 Total

Acknowledgements

The Center for Infrastructure Assurance and Security (CIAS) acknowledges the leadership and guidance of Salve Regina University's Pell Center for International Relations and Public Policy, and most especially Ms. Francesca Spidalieri. Francesca worked tirelessly to assemble representatives from across the Rhode Island corporate community and to provide a superb facility for the exercise, planning conferences and training sessions. Moreover, the CIAS recognizes the extraordinary support of Dr. James Ludes, Pell Center Executive Director. His vision and direct involvement were crucial in making this program a success. Finally, the CIAS greatly appreciates the expert support of Ms. Teresa Haas, Pell Center Office Manager. Teresa's hard work and attention to detail made all of the difference for this exercise.

SECTION 2: EXERCISE DESIGN SUMMARY

Exercise Purpose and Design

The purpose of this exercise was to bring Rhode Island corporate community leadership together to raise awareness and develop an understanding of cybersecurity and information sharing issues. This event was designed to demonstrate that the first steps in protecting organizations are opening lines of communication, implementing policies and procedures, establishing training and education programs and developing incident response plans.

A CIAS facilitator guided discussions at each table. They provided additional information and captured important issues and lessons learned from the scenario and the discussions. The facilitators submitted observations and comments that are included in this report.

Resources for this TTX and associated events were provided through funding from the Pell Center for International Relations and Public Policy at Salve Regina University.

Exercise Objectives

The objectives of this exercise were framed around the following issues:

- Cybersecurity Awareness
- Policies and Procedures
- Training and Education
- Information Sharing and Analysis
- Business Continuity
- Resiliency Planning

Scenario Summary

Overview

This exercise utilized fifteen events to allow participants to work through cybersecurity issues. It also focused on events that would likely promote information sharing. These issues reflected topics which the community felt were pertinent and relevant to their current challenges.

Storyline

A radical environmental and animal protection group has targeted organizations in the community. Their goal is to cause the greatest negative economic impact possible to stop contamination of the earth and its animals. This group operates under a leaderless model with no hierarchal structure. There are no official members or spokespeople for this organization, but the organization provides a banner for individual actions and leaves actions up to the actors' consciences.

The opening module included events that provided the up-front impact to participants. The module started with the local media at organizations asking questions about reports of a data compromise. From there, severe IT outages drove the need to prioritize resources to respond. The final event in the set-up was the notification that the organizational governing body wanted a report from senior management. From there the next two modules presented events as the day unfolded.

In the storyline during Module 1, leaders held a meeting with their staffs to determine the best course of action and to prepare a response for the next day's meeting with their governing body. During the meeting, several events were reported by various members of the staff to the leader. The IT security manager reported malicious software targeting the organization's antivirus software which caused systems to reboot. The database administrator reported that attackers gained access to databases with sensitive employee and customer data that were part of a new offering campaign. A social media site used by employees was compromised. The IT security manager also reported that email addresses and passwords from the compromise were posted on-line. The IT manager reported that spear phishing e-mails were received claiming users should login and provide their network ID and password for a new asset management tool. The physical security manager reported that five laptops and tablets were stolen over the past six months from various departments. The IT manager also recalled that an employee installed a wireless access point with security vulnerabilities on the corporate network.

In the second module, the antagonists leveraged attacks against the organization. They used the organization's network to attack other targets in order to cause confusion. Reports also suggested that attackers used social engineering to obtain more information about the internal workings of the organization, and obtained logins and passwords. A network administrator did not show up for work for four days. This departure aroused suspicions of a possible insider threat. The general counsel stated that a vendor reported a security breach that occurred 6 months ago. Later, an extortion threat was made by the antagonists to get money from their victims. At the end of the day, organizations in the community received bomb threats sent via email to their IT departments.

Below is a summary of the events in the exercise:

News media reports incident
Multiple computer systems crash
Reporting procedures
Overwhelmed IT resources
Data leakage and public disclosure
Social media and password re-use
Spear phishing emails
Laptops and tablets stolen
Rogue Wi-Fi
Another organization reports hacking attempts
Social engineering
Network administrator disappears
Third-Party vendor compromise
Extortion notice
Bomb threats emailed
Security controls bypassed with a "road apple"
Backup system found crashed
Child Exploitation Material discovered

Events Overview

Situation Set-up

News media reports incident

This event is designed to address media relations issues, proper procedures for public relations and employee training for speaking for their organization. This event also explores media responsibility and how media can affect the situation.

Multiple computer systems crash

This event is designed to address mitigation of malware infections and incident response. This event also explores identification of critical assets for business continuity and resilience planning.

Reporting procedures

This event is designed to address the reporting chain of command and to determine the cause of the incident and future mitigation strategy.

Module 1 Events

Overwhelmed IT resources

This event is designed to address disaster recovery and prioritization of systems and staffing. This event also explores identification of critical assets and team members for incident response purposes.

Data leakage and public disclosure

This event is designed to address issues associated with information leakage, data retention and destruction practices. This event also explores personnel training and awareness issues associated with public disclosure of employee and customer data loss.

Social media and password re-use

This event is designed to address social media usage policies and procedures. This event also explores a compromised password distributed on-line and the effects it can have on your organization if the employee re-uses the same password on your network.

Spear phishing emails

This event is designed to address phishing email, specifically those that solicit information from employees. This event explores social engineering, user awareness training, spoofed email and websites, and other tactics for spreading malware.

Laptops and tablets stolen

This event is designed to address risks associated with portable devices such as laptops, tablets and external media such as CDs, DVDs and USB drives. This event also explores data protection issues such as password protection and encryption.

Module 2 Events

Rogue Wi-Fi

This event is designed to address issues associated with wireless networks. This event also explores personnel training and awareness issues associated with open Wi-Fi networks.

Another organization reports hacking attempts from your organization

This event is designed to address response to penetration attempts originating from the participant's organization. This event also explores possible liability issues, network monitoring and egress security issues.

Social engineering

This event also explores social engineering techniques, specifically user awareness training and policies and procedures for information employees can give out over the phone. This event also explores Caller ID spoofing.

Network administrator disappears

This event is designed to address critical personnel, background checks and policies and procedures regarding an insider threat and missing employees. This event also explores separation of duties and single points of failure.

Third-Party vendor compromise

This event is designed to address the organization's reliance on third-party vendors and the associated risks. This event also explores information sharing related to third-party compromises.

Extortion notice

This event is designed to address the ability to work with law enforcement and respond properly to extortion attempts. This event also explores issues such as hoax identification, properly identifying email senders source, evidence preservation, executive support, legal support and incident response.

Bomb threats emailed

This event is designed to address how cyber issues can affect the physical world. This event also explores differences between cyber and physical procedures for addressing bomb threats.

Optional Events

Security controls bypassed with a "road apple"

This event is designed to address social engineering training and policies regarding "road apples" and removable media. This event also explores mass communication procedures and policies and incident response.

Backup system found crashed

This event is designed to address the importance of accurate backups in incident response. This event also explores backup testing, media rotation and offsite storage.

Child Exploitation Material discovered

This event is designed to address child exploitation material issues. This event also explores proper incident and evidence handling and law enforcement considerations.

Module Three Overview

- Table participants discussed the top three lessons learned
- Table spokespeople then shared their top three lessons learned with the entire group
- Participants filled out feedback surveys
- The Exercise Director ended the event with a final wrap-up

Exercise Structure

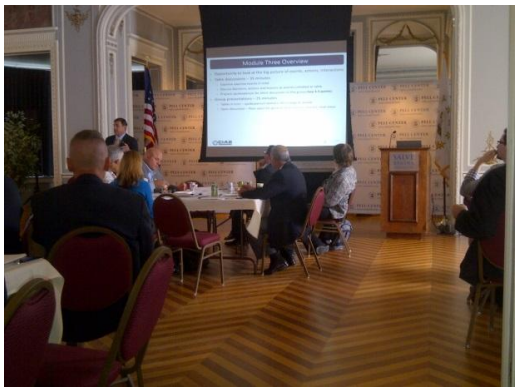
The exercise was divided into 3 modules preceded with a set-up.

Situation Set-up	presented events to drive subsequent actions in the exercise
Module One	presented events for leadership reaction
Module Two	presented the attack phase, which takes place over a 1-hour period
Module Three	allowed participants to share lessons in a guided discussion format

This page intentionally left blank.

SECTION 3: OBSERVATIONS AND RECOMMENDATIONS

This exercise is an effort to extend protection of critical infrastructures to the cyber world. The existing means to protect the community and respond to issues can be augmented by incorporating cybersecurity into processes and procedures. Many of these issues relate to other issues as they center around incorporating information sharing of cybersecurity events within organizations, across sectors and throughout the state.



Analysis Methodology

This event was a leadership awareness exercise that emphasized information sharing across sectors. The observations were taken from comments made during the exercise by participants as well as by facilitators at the tables. From there, the analysis condensed the lessons learned. The five main issues in this section are a product of that analysis. Many of the observations cut across multiple issues because the issues are related.

Issue 1.0: Management Buy-In

Leadership support is critical to the foundation of any information security program. Without buy-in and ownership by the leaders of the organization, the program cannot be successful. Developing this culture will help to focus the way people think and behave with regard to cybersecurity. Leaders that set the tone and actively promote the goals of the organization will cultivate this successful security culture.

Observation/Analysis 1.1: During the exercise, the leaders recognized the importance of their roles in effecting culture change. One participant, when reflecting on his next actions when returning to his organization, resolved that he was going to "not be complacent about the issue," realizing that he needed to "exert more energy and care about it." Another recognized that "culture change is not a set and forget" proposition. It takes leadership, understanding, and resolve to change the culture of an organization and it doesn't happen overnight.

Recommendations:

1. Demonstrate the importance of cybersecurity. One of the best ways to influence culture is by demonstrating over and over again what things are important to leadership. Leaders can do this through statements, through policies, and even through the questions they ask.
2. Sustain and enhance your organization's cybersecurity culture. To prevent security from becoming merely the flavor of the month, management needs to focus continually on cybersecurity. This means that cybersecurity should be a topic that is addressed at every quarterly meeting and every state of the company address. It needs to consistently be a topic of conversation.

Observation/Analysis 1.2: Participants discussed leadership's role in cybersecurity with one participant noting, "This is a C-level problem – IT can't own it – so it is a C-level solution." Another participant added, "For you to know when something bad is going on, you have to know the heartbeat of your business." This again highlighted management's role in cybersecurity for their organizations.

Recommendations:

1. Make cybersecurity part of the process of doing business. Cybersecurity needs to be integrated into every part of how the business operates. It is not sufficient for organizations to consider cybersecurity an IT issue, management must take responsibility for the impact that ineffective cybersecurity can have to the business.
2. Participate in the on-going Pell Center Initiative. The Pell Center has established a Rhode Island Corporate Cybersecurity Initiative designed to promote cybersecurity awareness and training, encourage information sharing and identify cybersecurity best practices. Seek out opportunities to collaborate with other cybersecurity initiatives from such organizations as the Rhode Island Economic Development Corporation. Initiatives like these can help organizational leadership own and address cybersecurity as a C-level problem.

Observation/Analysis 1.3: Organizations at the exercise understood that leadership is not just about providing direction but also about setting a good example. One participant stated, "Management enthusiasm for the topic can be infectious." He went on to note that under the right circumstances, when asked "staff and employees will eagerly offer solutions that work for them at no cost." This requires leadership that is excited about cybersecurity and promotes a culture where cybersecurity is important and everyone's responsibility.

Recommendations:

1. Lead by example. Leadership is not just about providing direction but also about setting a good example. If leaders don't have time for security or don't want to be bothered with strong passwords, it follows that employees will feel the same way.

Issue 2.0: Cybersecurity Awareness

Organizations need to develop a culture of cybersecurity awareness to focus on the way people think and behave with regard to cybersecurity. Leadership is the most important component of a cybersecurity program that fosters awareness. Awareness is a force multiplier that effectively turns every employee into a security barrier, the front line of defense, for their organization. When correctly implemented, cybersecurity awareness breeds a culture of cybersecurity vigilance that pervades the organization.

Observation/Analysis 2.1: At the exercise, participants expressed their agreement that cybersecurity awareness was important. One participant stated, "Organizational awareness has to extend all the way to the individual employee." Another said, "…cybersecurity needs to be intimate" indicating that employees have a direct impact on the security of their critical business practices.

Recommendations:

1. Senior leadership should demonstrate their commitment to a cybersecurity program and champion an effort that leaves everyone knowing where key resources and procedures exist for guidance.

Observation/Analysis 2.2: Discussions at the exercise also focused on sharing existing cybersecurity awareness resources. One person from the Rhode Island State Police indicated a need for a "Checklist for the public." In addition, people pointed out that the exercise was just the starting point. A participant said, "There is a need to support and promote awareness past the Pell exercise."

Recommendations:

1. The community should form a collaborative working group that can gather existing best practices from organizations and develop cybersecurity awareness resources.

Observation/Analysis 2.3: During the exercise, events highlighted the changing nature of critical business functions that have become increasingly reliant on computers and networks. This added urgency in the minds of participants for cybersecurity awareness programs throughout organizations in the Rhode Island Corporate Community. One participant who said, "The world has changed rapidly," indicating that technology has integrated rapidly with organizations and awareness was key to ensuring information remains secure. In support of that statement, another participant added, "We need to put things into context. We're in a frontier lacking resources."

Recommendations:

1. Leaders must ensure cybersecurity awareness programs remain updated and current with trends in personal and enterprise technologies.
2. Leaders would do well to dedicate resources for cybersecurity awareness programs and materials. Collectively, the community can assist organizations to expand the impact of cybersecurity awareness through scale of effort by many contributing to the effort.

Issue 3.0: Policies and Procedures

Policies are formal, brief and high-level statements or plans that embrace an organization's general beliefs, goals and objectives. Procedures describe an acceptable process for a specified subject area. Together they help arm organizations with guidelines and tools to address issues and situations that confront them.

Observation/Analysis 3.1: Cybersecurity policies don't have to be stand-alone documents. Participants at the exercise acknowledged that cybersecurity has to integrate with existing documents. In fact, one participant stated, "Everyone knows the physical drill but do we have a cyber drill?" This indicated that cybersecurty policies may lag behind other common organizational policies. To reinforce that issue, another participant stated, "Rules haven't caught up with policies."

Recommendations:

1. Review existing policies and identify gaps where critical business processes are supported with networks and computer systems.
2. Work to integrate cybersecurity into existing policies or create new ones, based on the organizational governance model.
3. Prioritize critical services and infrastructure. Conduct a dependency mapping activity to determine the priorities that can then be written into policies and procedures.

Observation/Analysis 3.2: Developing cybersecurity policies or modifying existing policies to include cybersecurity takes leadership and deliberate planning in the organization. One participant said, "You have to have a plan, it has to be practical and you have to have continuous improvement." Incorporating cybersecurity policies in the organization requires all stakeholders to be involved. This is reinforced by a comment made during the exercise where one participant said, "Collaborate with ALL, including third-parties."

Recommendations:

1. Identify the means by which policies are developed and approved in the organization. Include stakeholders from different parts of the organization including legal, compliance, physical security, operations and sales, as well as IT.
2. Establish a policy review program that is continuous and ensures cybersecurity is included in policy statements made by management.

Observation/Analysis 3.3: Several participants made note of including third parties in their cybersecurity policies and procedures Clearly there are organizations in the Rhode Island Corporate Community that take third parties into account. Third parties include vendors, partners and even customers. The community has the opportunity to help organizations share and collaborate on creating cybersecurity policies or integrating it into existing policies.

Recommendations:

1. Contractors and third-party vendors extend the boundaries of organizations. Just as a single employee can negate defenses that organizations have put in place, a single third-party vendor can cause just as much havoc. The policies that employees have to follow should also extend to contractors and vendors.

2. Include cybersecurity policies and procedures in third-party vendor contracts and audit vendor activities.
3. Organizations with cybersecurity policies can strengthen the community as a whole by sharing their policies with other organizations. Include the Pell Center in fostering a policies and procedures working group where organizations can collaborate on integrating cybersecurity into existing policies or create new ones.

Issue 4.0: Information Sharing

Information sharing is an integral part of an effective information security culture. Robust information sharing can improve resilience for the organization and the community. To be effective and mutually beneficial, information sharing should be reciprocal in nature. Information has to flow both to and from the organization, and to and from senior leadership and other members of the organization. One advantage is that the sharing of information is a force multiplier; it expands capabilities and improves incident response. Information sharing can be informal, semi-formal or formal.

Observation/Analysis 4.1: The value of information sharing was widely recognized across the exercise. One participant accurately captured the sentiment when he said, "Relationships are free and lucrative." Many participants even said that part of the value of the exercise was information sharing relationships that it helped to create. There were, however, some issues related to information sharing that participants felt needed to be addressed. One participant noted that organizations need to "know when to ask for help." Another participant observed, "There needs to be willingness for people to share information."

Recommendations:

1. Address barriers to information sharing. There are a multitude of real and perceived barriers given to justify not sharing information. Some barriers are valid and some are not. Review the reasons for withholding information. Have the courage to set aside the invalid reasons such as fear of reputation damage or a tradition of remaining silent. Determine mitigations or work-arounds for the valid reasons such as privacy and compliance issues.

Observation/Analysis 4.2: During the exercise participants discussed the types of information that should be shared and with whom. The consensus was that while information sharing was important, organizations still need to work on sharing information both internally and externally. Regarding internal information sharing, one participant said that there were occasions where IT "couldn't talk to the C-level" because "lingo and jargon" were barriers.

Recommendations:

1. Share information internally and externally. Consider who could benefit from receiving information. Internal divisions and users can better protect themselves and data if they are aware of threats and how to mitigate them. The partners and organizations relied on can be made more aware and thus more secure. They may even be able to help with internal issues if they have already dealt with those same issues.

Observation/Analysis 4.3: Organizations at the exercise generally wanted to share information with each other. There was sharing at the tables between participants at the same table and then among tables during the breaks and Module Three. Beyond the informal relationships, the Rhode Island Cyber Disruption Team noted that they were working on a collaborative tool that they might be able to share with other organizations. The Pell Center expressed its interest "in providing a cybersecurity hub."

Recommendations:

1. Identify partners for information sharing. Again, consider who could benefit from shared information, but also who could be the source of valuable information. Consider partnering with these organizations, as well as those involved in maintaining the security of our wider community.
2. Establish formal information sharing agreements. One of the best ways to overcome barriers to information sharing is to draw up Memoranda of Understanding (MOU), Non-disclosure agreements (NDA) and Memoranda of Agreement (MOA) before incidents occur, and then testing and drilling to practice and find gaps or issues.

Issue 5.0 Training and Education

Because people are often the weakest link in any cybersecurity program, it is important to invest in personnel training, particularly for those that have cybersecurity as a primary responsibility. Training and education can also help enable culture change. They provide conduits for leadership to get their message to employees. Through training and education, organizations can take the weakest link – personnel – and turn them into a cybersecurity "front line," making them more effective in detecting and defending against cyber issues. It becomes an investment in the organization's cybersecurity.

Observation/Analysis 5.1: Participants generally recognized the importance of training and education with respect to cybersecurity. One participant summarized, "We need educated end users." While another emphasized, "Educate, Educate, Educate!"

Recommendations:

1. Train and educate workforce and staff. Every person in the organization can be either a weak link or a cybersecurity guard. Engage every person in cybersecurity to makes them all cybersecurity guards.

Observation/Analysis 5.2: During the exercise, participants noted that the cyber threat is constantly changing and that training programs must keep up with those changes. Specifically a participant mused, "It's no longer script-kiddies in the basement." To stay on top of these changing threats we cannot depend only on IT to protect the infrastructure. We have to "teach users to be curious about anomalies," said one participant. Users can become part of the early warning system to help detect threats before they become problems. This can only happen if we empower and motivate users to be part of the solution.

Recommendations:

1. Ensure that training is personal and relevant. As with awareness, when participants feel training is relevant to their personal welfare both on and off the job, they are more motivated to learn, and more motivated to implement what they learn. To be effective, training must happen on a regular basis, and must engage the participants.
2. Allocate resources to training. Training often takes a back seat to other business demands. It may be difficult to justify spending resources on training when it rarely has an obvious direct effect on the bottom line. However, when regarded as an investment that will decrease incident costs and will yield returns in the long run by improving workforce morale and capabilities, dedicating resources to training makes more sense.

Observation/Analysis 5.3: A great deal of expertise exists within the state of Rhode Island regarding cybersecurity and incident response in both the public and private sectors. Several participants offered to share or look into sharing resources that their organizations had. For example, one participant had a cyber-range that could potentially be shared with others, while another offered a gaming platform called Mutual Fun that others might be able to leverage.

Organizations can identify these resources and gather them together with the intent to share across the state. Cybersecurity training and education will aid organizations in strengthening their enterprises and thus better protect their critical infrastructure.

Recommendations:

1. Pool resources and work together. Consider cooperating to share the expense of training across departments, organizations and even the community. Offer existing resources to other organizations and take advantage of resources made available by other organizations. Organizations can leverage economies of scale to reduce the costs associated with training of personnel. When organizations pool their resources, they can bring a single instructor on-site instead of sending multiple personnel away.

SECTION 4: CONCLUSION

The purpose of this exercise was to provide leadership the opportunity to raise their awareness and develop an understanding of cybersecurity threats and issues. The participants dealt with real-world cybersecurity issues and events designed to promote incident response and information sharing between organizations. Thirty people represented their respective organizations. Participants were encouraged to talk through the issues, discuss how they believed their organization would handle the situations and identify any related best practices.

The participation and interaction at the exercise displayed a distinct and identifiable cohesiveness among the participating organizations. The exercise allowed senior leadership in Rhode Island to share the lessons they learned about cybersecurity with colleagues and counterparts. Participants were able to gain insight from each other's perspectives and their discussions demonstrated a resolve to increase cybersecurity awareness among employees and to share information with key partners. These insights and discussions are basis for many of the recommendations in this report.

Additionally, the CIAS further recommends the following actions to reinforce and facilitate the implementation of many of the recommendations of this report.

- Conduct *additional tabletop exercises*. Consider the following categories:
  - Public-Private Partnership Tabletop: Conduct an exercise similar to the Corporate Community Cybersecurity Tabletop and expand the size and scope to include public sector partners and their senior leadership. Develop an awareness of the necessity and the ability to protect the citizens and infrastructure of Rhode Island.
  - Information Sharing Tabletop: This exercise can build on the raised awareness and developed relationships of the first activity while emphasizing the sharing of information before, during and after a cyber-event. Provide participants the opportunity to actively share information in and out of their sector and business areas. Explore what specifically can and would be shared, when and how.
- Provide *disaster response and recovery workshops and training* as a follow-up to the above exercises. Cultivate the interest generated during the exercises into concrete action in responding and recovering to cyber incidents.
- Perform *organizational risk workshops* to assist participants in better understanding their organization's operations .
- Collaborate in *dependency mapping* activities to determine, and in some cases, uncover, organizational dependencies, both internal and external.
- Work together to offer robust *workforce development* through mentoring, internships, and the sponsoring training and certification activities in cybersecurity.

In conclusion, key leaders were enthusiastic and very interested in leveraging the exercise discussions and lessons learned. These organizations are well positioned to build on these relationships to better protect their employees and their critical infrastructure. Continued involvement in the Pell Center Initiative and other collaborative activities will continue to strengthen the Rhode Island Corporate Community.

APPENDIX A: IMPROVEMENT PLAN

The Cybersecurity Framework (illustrated above) depicts a five-part process for establishing a cybersecurity program within an organization, community or state. As is the case for many large programs, senior leadership (management) support is paramount to success. In the context of cybersecurity, leadership should "champion" stated goals and objectives. Stakeholder awareness of policies and procedures is the next step, and requires both strategic and tactical thinking in order to guarantee success. Once management has expressed its support, policies and procedures should be written to address identified issues and concerns. Training employees and citizens alike is a necessary step towards accomplishing a level of information sharing that is beneficial to all.

The Cybersecurity Framework is derived from a number of industry-standard information security controls including National Institute of Standards and Technology (NIST) Special Publication 800-53, Control Objectives for Information and Related Technology (COBIT) and the Information Technology Infrastructure Library (ITIL). The Center for Infrastructure Assurance and Security has combined the control sets and categorized them in order to provide states and communities with a starting point.

APPENDIX B: LESSONS LEARNED

Appendix B is not applicable for this After Action Report.

APPENDIX C: PARTICIPANT FEEDBACK SUMMARY

Feedback Form

Please circle the most appropriate response.								
Please choose your organization's industry:	Government (Local/State/Fed)	Private Sector	Military					
				1	2	3	4	5
				Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
If this event involved a moderator, the moderator effectively presented and managed the event.				1	2	3	4	5
The event session and materials were well organized.				1	2	3	4	5
The presentation was clear and understandable.				1	2	3	4	5
The instructor/facilitator was well prepared and knowledgeable.				1	2	3	4	5
The instructor/facilitator encouraged questions.				1	2	3	4	5
The examples helped clarify the instruction.				1	2	3	4	5
This event increased the group's understanding of cyber security.				1	2	3	4	5
This event increased my understanding of the need for community interaction and cooperation.				1	2	3	4	5
This event raised relevant issues about the community's ability to interact in an actual emergency/disaster/incident.				1	2	3	4	5
The information I received can be put to practical use.				1	2	3	4	5
The facilities' conditions were conducive to learning.				1	2	3	4	5
I enjoyed the food and refreshments and they were provided at logical break points.				1	2	3	4	5
Additional Comments (use reverse if necessary)								

Rhode Island Corporate Community Cybersecurity Tabletop Exercise
Feedback Results
October 9, 2013

Please circle the most appropriate response.

Please choose your organization's industry:	Government (Local/State/Fed)	Private Sector	Military

	1 Strongly disagree	2 Disagree	3 Neither agree nor disagree	4 Agree	5 Strongly agree
If this event involved a moderator, the moderator effectively presented and managed the event.				**4.89**	
The event session and materials were well organized.				**4.81**	
The presentation was clear and understandable.				**4.82**	
The instructor/facilitator was well prepared and knowledgeable.				**4.89**	
The instructor/facilitator encouraged questions.				**4.79**	
The examples helped clarify the instruction.				**4.54**	
This event increased the group's understanding of cyber security.				**4.77**	
This event increased my understanding of the need for community interaction and cooperation.				**4.62**	
This event raised relevant issues about the community's ability to interact in an actual emergency/disaster/incident.				**4.59**	
The information I received can be put to practical use.				**4.73**	
The facilities' conditions were conducive to learning.				**4.81**	
I enjoyed the food and refreshments and they were provided at logical break points.				**4.76**	

Breakdown of Feedback Results

The feedback form contained essentially two types of information. The first addressed the participants' perception of cybersecurity, while the second concerned their perceptions of the effectiveness of the CIAS training. Figures 1 and 2 represent those differences. The graphs are scaled to show response levels 3 through 5, as all of the surveys showed a general appreciation of the event.

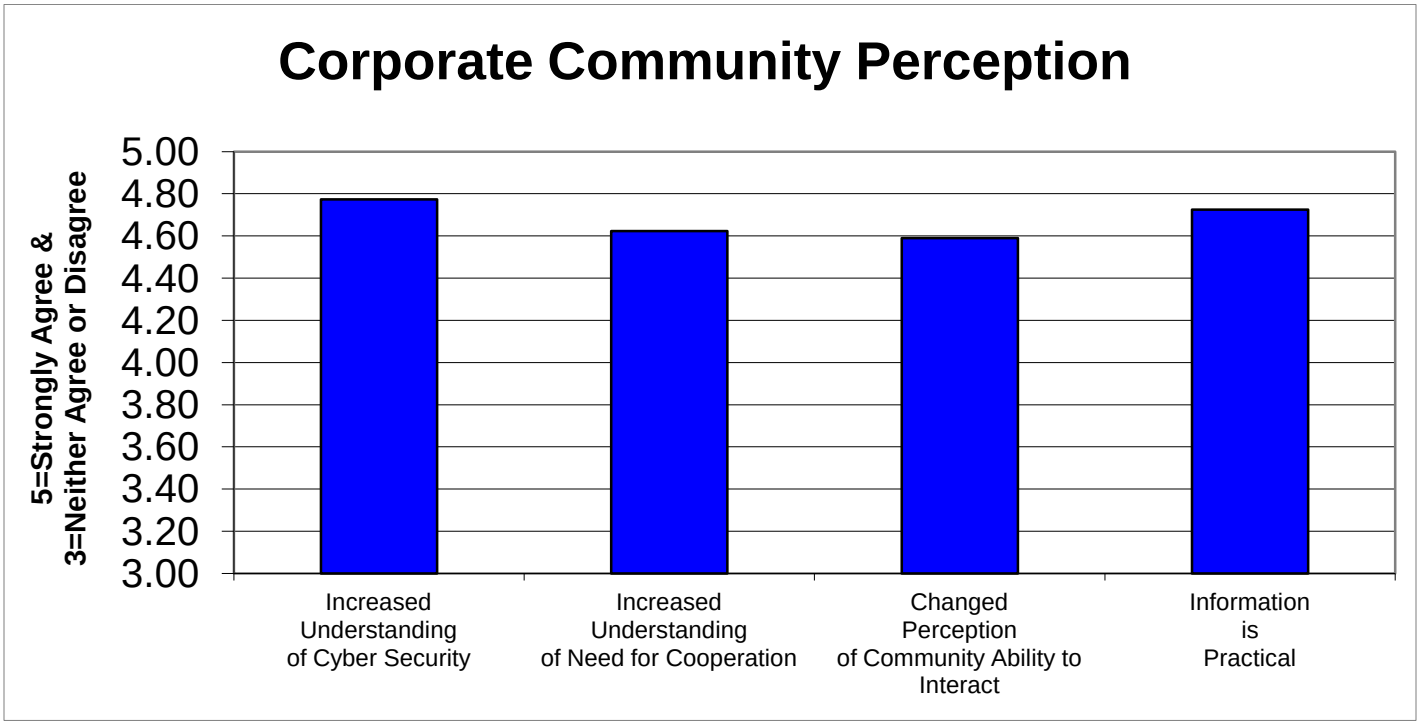


Figure 1 Questions Dealing with State and Community Perception

Overall, participants indicated that the TTX increased their understanding of cybersecurity and underscored the need for information sharing throughout the community. Most participants stated that the exercise changed their perception of the ability to interact during an incident and felt they gained practical information from the exercise.

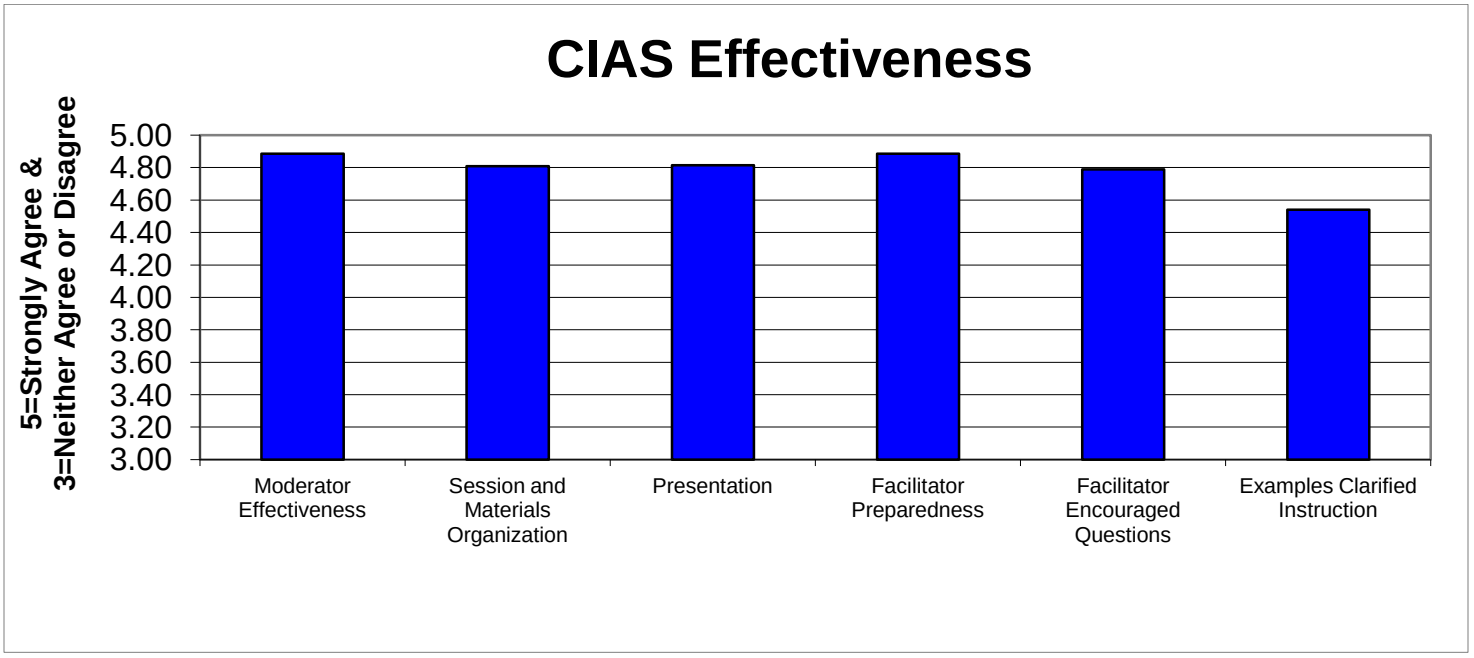


Figure 2 Questions Dealing with CIAS Presentation Effectiveness

This figure represents the perception of the effectiveness of the presentation and facilitation performed by the CIAS. Overall, responses indicate the community strongly agrees that CIAS' program and personnel were highly effective in presenting the materials and facilitating discussions.

APPENDIX D: TTX EVENTS SUMMARY TABLE

Date	Time	Event
Wednesday, October 9, 2013	9:00 AM	News media reports incident
Wednesday, October 9, 2013	9:15 AM	Multiple computer systems crash
Wednesday, October 9, 2013	10:00 AM	Reporting procedures
Wednesday, October 9, 2013	10:30 AM	Overwhelmed IT resources
Wednesday, October 9, 2013	10:42 AM	Data leakage and public disclosure
Wednesday, October 9, 2013	10:55 AM	Social media and password re-use
Wednesday, October 9, 2013	11:08 AM	Spear phishing emails
Wednesday, October 9, 2013	11:20 AM	Laptops and tablets stolen
Wednesday, October 9, 2013	11:32 AM	Rogue Wi-Fi
Wednesday, October 9, 2013	12:15 PM	Another organization reports hacking attempts
Wednesday, October 9, 2013	12:27 PM	Social engineering
Wednesday, October 9, 2013	12:40 PM	Network administrator disappears
Wednesday, October 9, 2013	12:52 PM	Third-party vendor compromise
Wednesday, October 9, 2013	1:10 PM	Extortion notice
Wednesday, October 9, 2013	1:20 PM	Bomb threats emailed

APPENDIX E: PERFORMANCE RATINGS

Appendix E is not applicable for this After Action Report.

APPENDIX F: ACRONYMS

Acronym	Meaning
AAR	After Action Report
CCSE	Community Cybersecurity Exercise
CIAS	Center for Infrastructure Assurance and Security
COBIT	Control Objectives for Information and Related Technology
ID	Identification
IP	Improvement Plan
IPC	Initial Planning Conference
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NDA	Non-disclosure Agreement
NIST	National Institute of Standards and Technology
POC	Point of Contact
TTX	Tabletop Exercise