
Wisconsin Cyber Disruption Response Strategy



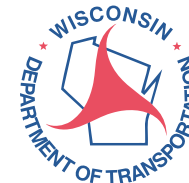
Protecting Critical
Infrastructure and
Systems of
Wisconsin



WISCONSIN DEPARTMENT OF
ADMINISTRATION

**Milwaukee
Water Works**

Safe, Abundant Drinking Water.





**State of Wisconsin
Homeland Security Council**

SCOTT WALKER
Governor

MAJ GEN DONALD P. DUNBAR
Homeland Security Advisor

Department of Military Affairs
2400 Wright Street
Madison, WI 53704
(608) 242-3075

October 30, 2015

Dear Wisconsin Critical Infrastructure Partners:

Wisconsin government detects millions of unauthorized attempts to probe, scan and access or disrupt its computer networks. These same computer networks safeguard important information about Wisconsin's residents, control critical state agency operating systems, and provide our customers with convenient access to state services. While the vast majority of these cyber anomalies are blocked by defensive systems, evolving threats represent a significant risk to the continuity of state government. Similar challenges are faced by Wisconsin's private sector and local government partners, all of whom are also working diligently to safeguard their systems.

With the understanding that it takes a network to protect a network, we initiated an effort to encourage a statewide collaboration among public and private partners to defend Wisconsin's critical networks. In support of this initiative, a team of state and local government representatives and private sector critical infrastructure owners and operators have developed the Wisconsin Cyber Disruption Response Strategy. Each organization is represented in the 16 Critical Infrastructure and Key Resource (CIKR) Sectors as defined by the Department of Homeland Security.

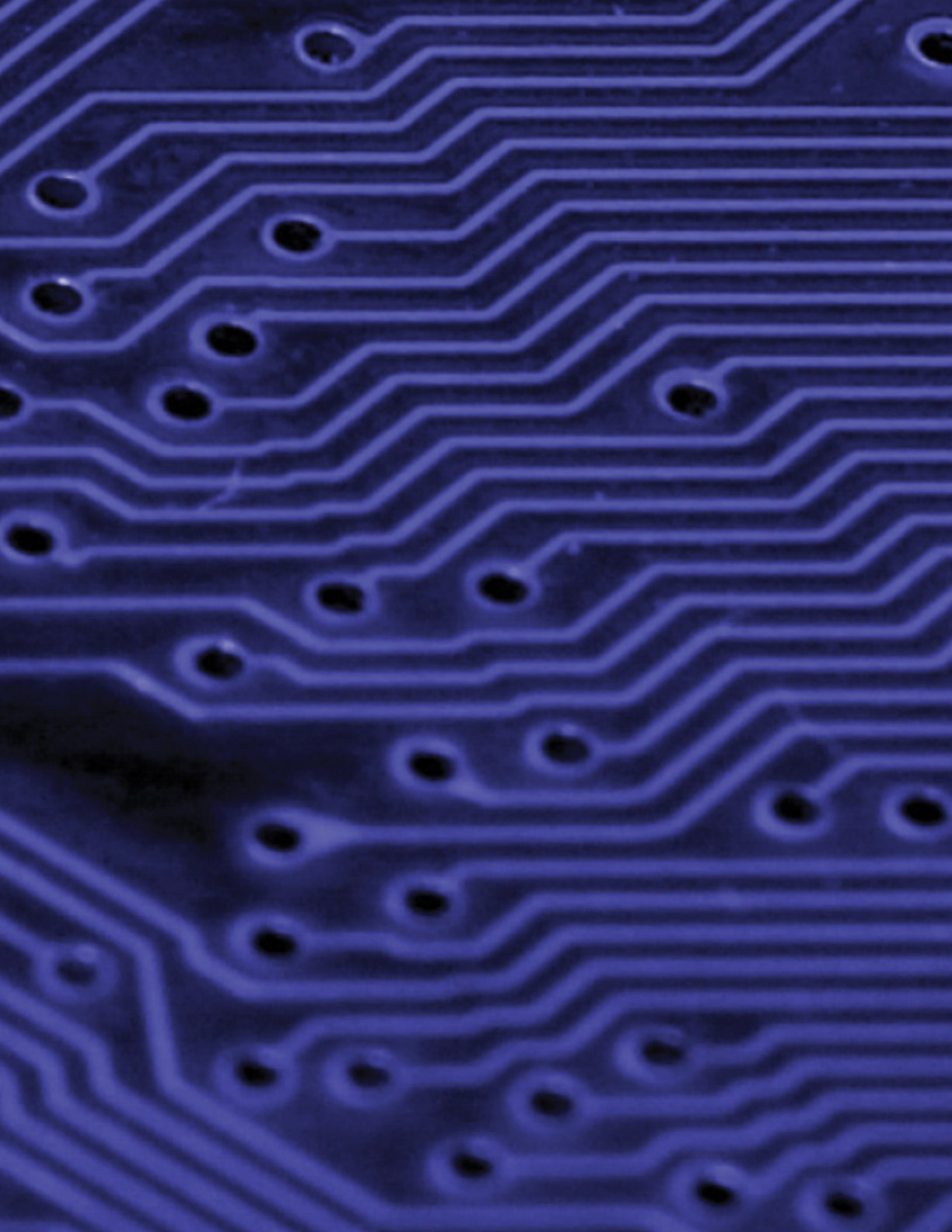
This document provides a framework to first identify cyber attacks, then protect, detect the threat, respond to and recover from a significant cyber disruption to Wisconsin's critical infrastructure. Through the strategy and its operational annexes, participating organizations can collaborate in response to cyber threats either before or after they occur. The strategy sets forth five goals and objectives designed to provide an operational framework to respond to today's cyber anomalies, as well as a cooperative approach aimed at preparing and maintaining a cadre of cybersecurity partners to maintain ongoing readiness.

In 2016, the cyber disruption response strategy team will develop an overall strategic plan that will focus on training and full scale exercises for our private and public sectors. This full scale training initiative will link our IT professionals together and strengthen our readiness for a cyber disruption.

It is our hope that by unifying state government cybersecurity efforts, and by working closely with our private sector and local government partners, we can continue Wisconsin's role as a national model of innovation, success and security.

DONALD P. DUNBAR
Maj Gen, Wisconsin National Guard
The Adjutant General & WI Homeland Security Advisor

David Cagigal
Chief Information Officer
State of Wisconsin



Contents

Introduction	2
Goals, Objectives, and Performance Measures	3
Implementation, Management, and Operations	8
Conclusion	10
Communication Annex	12
Risk Assessment Annex	15
Response Plan Annex	21
Training & Exercise Annex	25
Representatives by CIKR Sectors	31

Introduction

Formation of the Wisconsin Cyber Disruption Response Strategy

The Wisconsin Cyber Disruption Response Strategy provides a framework to assist critical infrastructure owners and operators in the development of a collaborative, public and private partnership to respond to cyber disruption events affecting the State of Wisconsin. This strategy was developed by representatives from the 16 critical infrastructure sector owners in the State of Wisconsin, and state and local government officials. The overall intent of this framework is to limit the impact if the state had a cyber disruption, and in turn maintain critical services to the public.



Goals, Objectives, and Performance Measures

GOAL 1 - Governance Authority

Objective 1.1: To establish a cyber disruption response governance authority and strategy with one individual per main sector to ensure that all critical activities are governed among the critical infrastructure sectors below:

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

Objective 1.2: The governance authority of the following sectors will represent the 16 critical infrastructure sectors to achieve a consistent approach to the cyber disruption response planning process:

- Communications
- Emergency Services
- Energy
- Information Technology
- Nuclear Reactors
- Government Facilities
- Banking and Finance
- Transportation Systems

Objective 1.3: The governance authority will establish decision points mapped to the lifecycle of an event and determine the threat level, action plans and resource allocations.

GOAL 2 - Organization, Roles, and Processes

Objective 2.1: The governance authority serves as a forum of subject matter experts specifically charged with the responsibility, for each sector, to prepare for, respond to, and recover from a large-scale or long-duration cyber disruption that impacts the state, including the following:

- Intentional threats (e.g., terrorism)
- Cascade failures from inadvertent disruptions (e.g., backhoe work near utility lines)
- Events with natural causes (e.g., ice and coastal storms)

Objective 2.2: The process will overlay the roles and responsibilities map with the defined functions, processes and operating procedures between all members of the organization listed in cyber disruption governance. Each sector will map the following: Identify, Protect, Detect, Response, and Recovery.



GOAL 3 – Risk Profile and Capacity

Objective 3.1: Conduct thorough risk profiles to identify the vulnerabilities of Wisconsin's critical infrastructures to cyber attack.

Objective 3.1.1: A representative from each critical infrastructure will develop a risk profile and identify key resources of its networks by October 1, 2015.

Objective 3.1.2: Develop a remediation plan based on the risk profile priorities by December 31, 2016.

Objective 3.1.3: Identify and incorporate relevant cyber elements from existing state IT security plans, emergency management annexes, homeland security plans, disaster recovery plans, industry and service related plans.

Objective 3.1.4: Apply resources to the remediation of identified vulnerabilities and report outcomes by 2017.

Objective 3.1.5: Re-evaluate risk profiles for all sectors every 3 to 5 years.

GOAL 4 - Communications

Objective 4.1: Improve communication among cooperating critical infrastructure owners and operators through enhanced communications and collaboration regarding cyber threats.

Objective 4.1.1: Create a contact list of all participating critical infrastructure owners and operators by September 1, 2015.

Objective 4.1.2: Develop a system, agreed to by all parties, to share information among members by October 1, 2015.

Objective 4.1.3: Coordinating a response communication among key actors is integral to operational coordination to deal with primary and secondary effects, and cross-jurisdictional partnering. States should conduct the following:

- Develop a communications protocol integrated with cross-functional process flows, potentially through an existing or planned joint information center that will exist for the duration of a cyber disruption.
- Establish alternative means for enabling communications in case certain technologies (e-mail, phone, and public safety communications) are unavailable.

Objective 4.1.4: Develop a public information communication and education plan. This will raise awareness across state agencies and private partners regarding the current threat landscape, the interdependencies of infrastructures, and the necessity of developing effective strategies for cyber disruption response plans.

GOAL 5 – Response Recovery

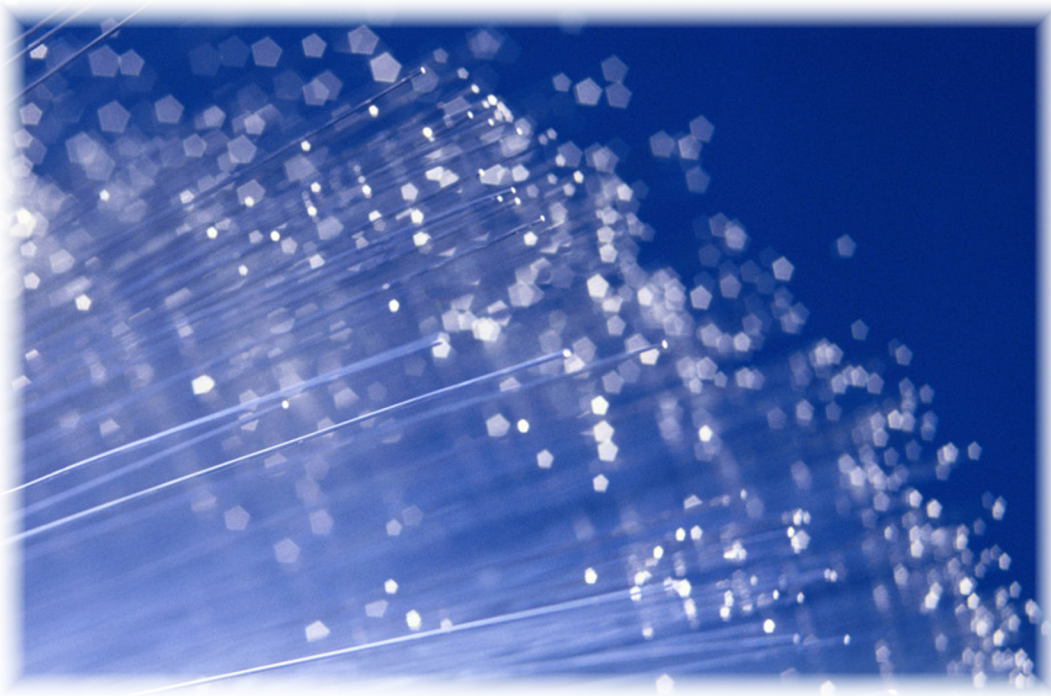
Objective 5.1: Train key staff and exercise communication and response plans developed in accordance with this strategy annually, beginning in 2015.

Objective 5.1.1: Develop a consensus-driven training plan for members and operators by 2016.

Objective 5.1.2: Develop an exercise plan for implementing the strategy by 2016.

Objective 5.1.3: Conduct exercises of at least one component of the cyber disruption strategy annually.

Objective 5.1.4: Deploy expert personnel who are prepared with the know-how and the tools necessary to maintain a high level of threat awareness, quickly detect and mitigate vulnerabilities, and minimize the consequences of cyber disruptions.





Implementation, Management, and Operations

The Wisconsin Cyber Disruption Response Strategy was formed and designed to serve as an ongoing framework for the private and public sectors to collaboratively respond to significant cyber events.

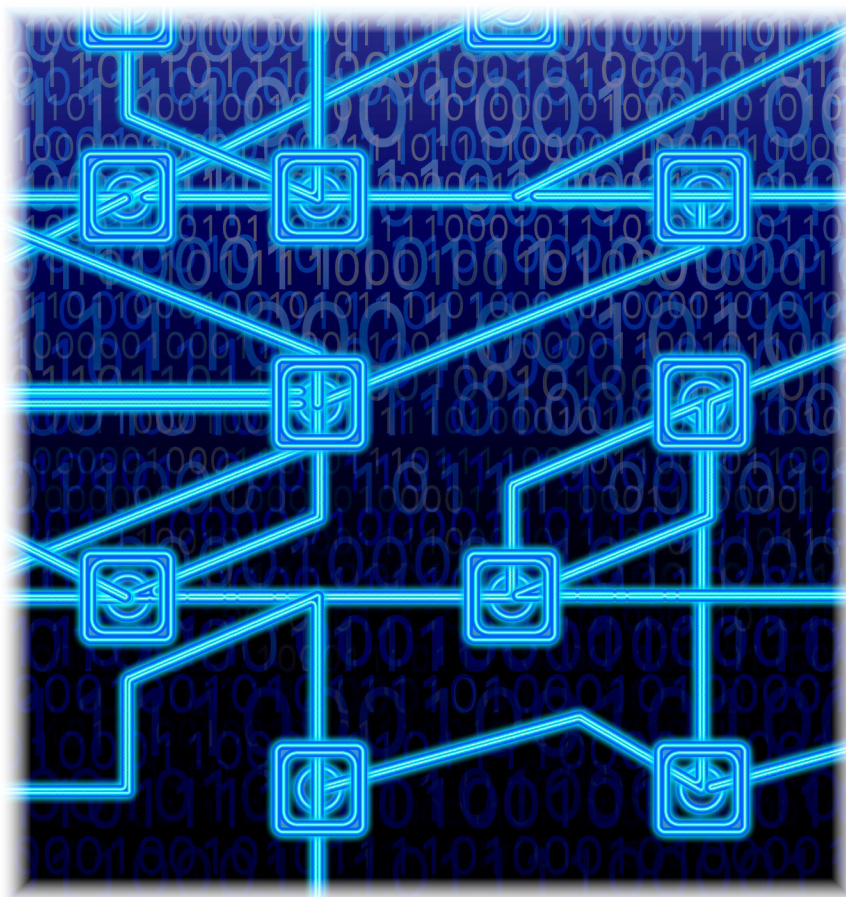
The strategy will continually evolve, and be the primary component to an ongoing development of specific plans for prevention of, response to and recovery from significant cyber disruptions. As a first priority, the governance will develop a written plan for communication during cyber events.

Initially, the group will develop the content of the first annex, the Communication Annex, which will provide the necessary framework for communication among all critical infrastructure owners and operators and government within Wisconsin. The Communication Annex will include the protocols for communicating among the sectors, as well as the governance, to mitigate the effects of cyber disruption. Following the completion of the first annex, strategy participants will develop specific plans for their response to cyber disruptions affecting their critical infrastructure.

As part of this planning process, critical infrastructure owners and operators will collaborate to identify specific interdependencies that exist within their respective sectors. In doing so, the unique vulnerabilities associated with these sectors will be identified and plans developed to address interdependencies as a key component of the planning process. To ensure that protected critical infrastructure information is not released, information must be safeguarded. As such, the annex may contain references to documents that are privately held by individual members and not available for public distribution with the strategy.

The second annex addresses the foundational need to understand the risk associated with cyber disruptions to critical facilities. An improved understanding of the threats, vulnerabilities and potential consequences of cyber disruptions to Wisconsin's critical infrastructure will result in more effective scenario-based response plans. Any cyber event that has the potential to substantially affect the State of Wisconsin, its residents, businesses or government, may result in the implementation of local or state emergency management plans.

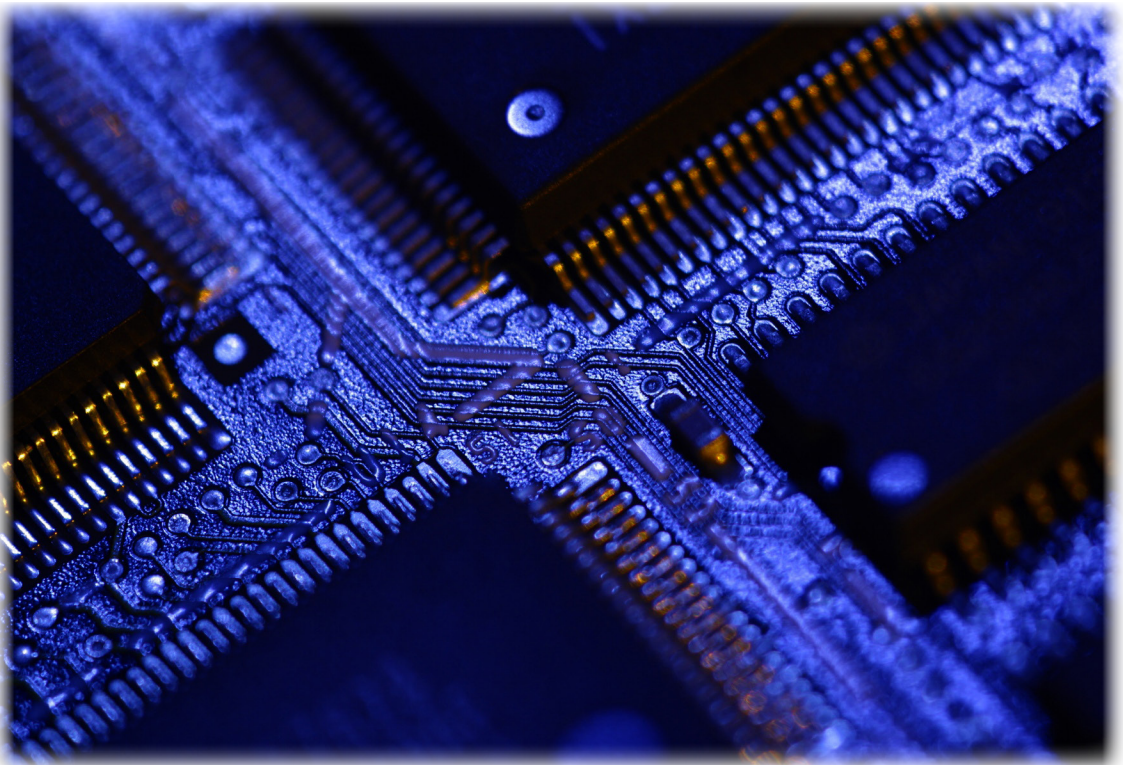
The final annex will provide specific training recommendations for the sectors of the strategic partnership with employees active in cyber disruption mitigation. These training recommendations will be customized for individual positions and their core competencies related to cybersecurity. In addition, the third annex will contain an exercise plan for the overall strategic initiative which will begin with drills and tabletop-level exercises in 2016, and culminate in a full scale exercise within two years.



Conclusion

Critical infrastructure systems are networks, and so are the groups that attack them. It follows that the best way to respond is to develop a network designed to protect critical infrastructure. Since it is not possible to protect every component of every network, efforts must be undertaken to protect the “critical nodes” identified through careful risk assessment and collaborative analysis of interdependencies.

The Wisconsin Cyber Disruption Response Strategy is our first step in the development of a force-positive network designed to apply risk-based mitigation strategies to the defense of critical infrastructure. The subsequent steps will be the detailed development of the plan and procedures to assess risk, communicate threats, issue protocols and train and exercise staff in the protection of Wisconsin’s critical infrastructure from significant cyber disruptions.





Communication Annex

Communication Annex

Introduction

The Wisconsin Statewide Information Center (WSIC) works in partnership with the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), as well as partners from other federal, state and local agencies and the private sector. In response to the emerging threats from cyber intrusions and associated disruptions, the WSIC has taken on roles and responsibilities in gathering, receiving, analyzing and disseminating cyber threat information.

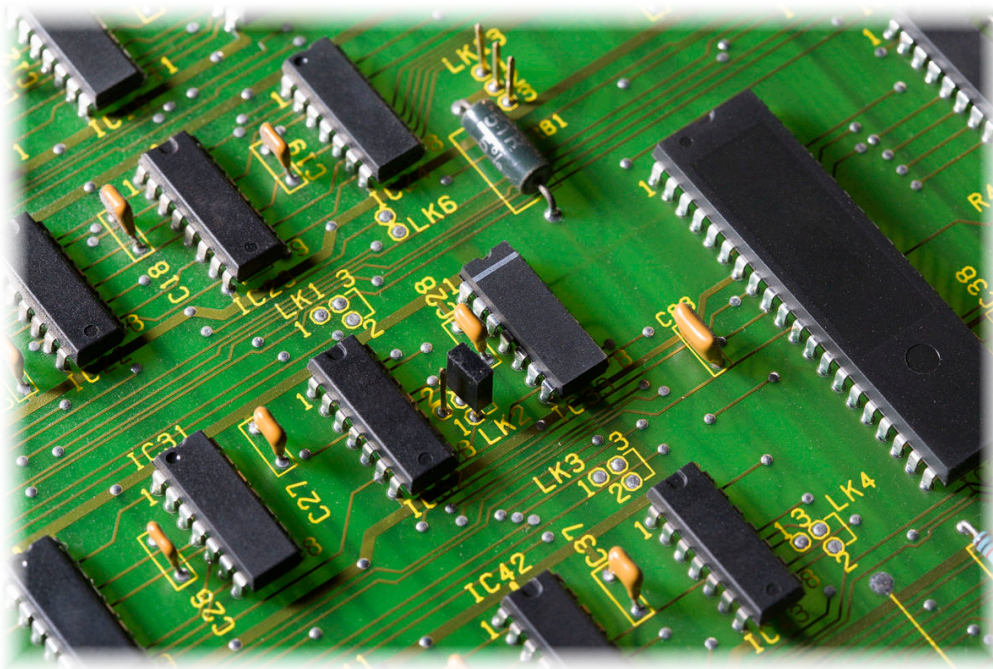
The WSIC gathers cyber threat information through partnerships with the private sector as well as state and local agencies. The WSIC Threat Liaison Officer (TLO) and Fusion Center Liaison Officer (FLO) programs are statewide initiatives to work with federal, state and local agencies as well as the private sector to provide training and serves as a mechanism for those TLOs and FLOs to submit suspicious activity reports (SARs) to WSIC in order to detect, prevent and respond to both criminal and terrorism related activities.

The WSIC receives cyber threat information from a variety of sources. The sources include:

- Department of Homeland Security (DHS)
- FBI
- Private sector
- State, local and tribal agencies
- The National Network of Fusion Centers
- Information Sharing and Analysis Centers (ISAC)
- Center for Internet Security and the Multi State Information and Analysis Center (MS-ISAC)
- Critical Infrastructure (CI) owners and operators
- Other federal agencies
- Open source

The WSIC analyzes information it gathers and receives. Analysts within the WSIC Intelligence and Analysis Unit (IAU) and partners within the fusion center analyze cyber threat information to determine the potential threat to critical infrastructure, private sector companies, the citizens of Wisconsin and the nation. In addition, WSIC analysts contribute to and utilize cyber threat analysis from across the National Network of Fusion Centers to provide the most comprehensive threat picture.

WSIC disseminates cyber threat information through its robust distribution network. Intelligence is disseminated both for situational awareness and for specific threats to critical infrastructure or other key resources (CIKR). Through the implementation of the governance authority of this strategy, WSIC will utilize the subject matter experts or “authorized agents” identified for each of the CIKR sectors to disseminate cyber threat intelligence.





Risk Assessment Annex

Risk Assessment Annex

Introduction

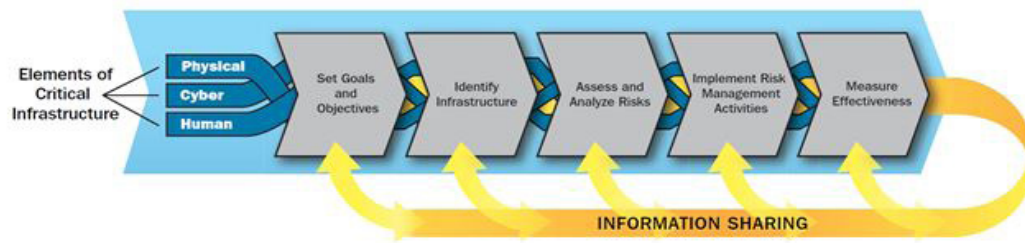
Wisconsin's critical infrastructure systems are vast, interconnected, interdependent networks. No single entity, public or private, can afford to apply the resources necessary to eliminate all threats to continuity. A public-private partnership, like that represented by the Wisconsin Cyber Disruption Response Strategy, can leverage the resources of multiple stakeholders to gain advantage, but even this falls short of total risk elimination. These limitations require the development of a method to assess and prioritize risks in order to focus resources on the most critical areas of Wisconsin's networks. This annex provides a framework for the assessment and management of the risk of disruption of Wisconsin's critical infrastructure networks.

Security and resilience are strengthened through risk management. Risk refers to the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences;" risk management is the "process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost."¹

Risk Management Framework

The National Infrastructure Protection Plan (NIPP) was developed by the US Department of Homeland Security as a strategy for the protection of national critical infrastructure. Within the NIPP, a risk management framework has been established to provide a common operational picture for the management of risk to critical infrastructure. The State of Wisconsin supports the National Infrastructure Protection Plan. The state-level risk management strategy builds upon this foundation and the overall tenets of the national plan.

The adopted risk management framework for the Wisconsin Cyber Disruption Response Strategy is represented in the following graphic²:



Each step of the framework is a key component of Wisconsin's overall cyber disruption risk management strategy. The Wisconsin Cyber Disruption Response Strategy sets goals and objectives for the management of cyber disruption affecting critical systems and incorporates many of the same concepts as the Michigan Cyber Disruption Response Strategy³. The remaining areas of the risk management framework are equally important to the effective management of cyber disruption risk.

Identification of Network Components and Cross-Sector Interdependencies

The first step in the assessment of risk to critical networks is the identification of the network components or assets. The development of a representative inventory of logical infrastructure and identification of the interconnected components of a network are necessary to understand the associated threats and vulnerabilities. The asset's position, connectivity, and other unique characteristics relate directly to their criticality and vulnerability.

Growing interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. For example, all critical infrastructure sectors rely on functions provided by energy, communications, transportation, and water systems, among others.

¹ U.S. Department of Homeland Security, DHS Risk Lexicon – 2010 Edition, September 2010

² U.S. Department of Homeland Security (2009) National Infrastructure Protection Plan (NIPP). Washington, DC

³ Michigan Cyber Disruption Strategy (2013)

In addition, interdependencies flow both ways, as with the dependence of energy and communications systems on each other and on other functions. It is important for the critical infrastructure community to understand and appropriately account for these interdependencies when managing risk.

Risk Assessment Methodology

Risk assessment involves the development of a measure of risk based on the evaluation of the threat, vulnerability and consequence associated with an attack on a target, such as critical infrastructure. Critical infrastructure risks can be assessed in terms of the following:

- Threat – natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- Vulnerability – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- Consequence – effect of an event, incident, or occurrence.

Common methods for risk assessment include the use of subject matter experts and the scoring of risk characteristics based on relativistic scales. Each of the sectors has unique requirements and constituencies and conduct risk assessments to inform their own decision making. The Wisconsin Cyber Disruption Response Strategy does not mandate a specific risk assessment methodology. Instead, a standardized risk profile leverages the risk assessments performed for critical infrastructure owners/operators to enable information sharing related to common vulnerabilities, threat intelligence and response strategies across sectors. It is expected that risk profile discussions from a representative sample of industries will identify interdependencies, improve information sharing, and assist in the identification of key risks and threats to Wisconsin's critical infrastructure.

Prioritized Remediation

The goal of the risk assessment process is to provide a prioritization of the critical assets of Wisconsin's networks, a plan to safeguard them and identification of interdependencies.

The highest priority assets should be those that are most vulnerable, have the greatest impact to the public, or impact other critical infrastructure sectors if disrupted. As such, these critical nodes should receive the greatest amount of resource support. Members will develop remediation plans based on their risk assessment activities by December 31, 2015. Key aspects of these plans will be shared with the partnership at a level of detail deemed appropriate by the reporting member.

It is envisioned that, where possible, partners of the Wisconsin Cyber Disruption Response Strategy will share relevant information about their highest priority assets. The identification of critical nodes within Wisconsin's critical infrastructure networks will allow the State of Wisconsin and its partners to better coordinate resources to assist in protecting critical systems and responding to incidents. Additionally, training and exercise programs can be tailored to target the protection of these critical assets and identify parties involved in incident response efforts.

Measuring Effectiveness

An effective risk assessment program should yield measurable progress. Regular meetings of the Wisconsin Cyber Disruption Response Strategy Partners held after 2015 (when remediation and communication plans are developed) will include a structured report of the effectiveness of remediation. These reports will include, at minimum, a total number of successful disruptions and a measurement of any applicable reductions in disruptions of critical networks associated with the remediation activities undertaken.

Enable Risk-Informed Decision Making

To ensure that situational awareness capabilities keep pace with a dynamic and evolving risk environment, the Wisconsin critical infrastructure community should continue to improve practices for sharing information and applying the knowledge gained through changes in policy, process, and culture. The community can promote a culture of “need to share” and “responsibility to provide” across all levels and sectors, recognizing that critical infrastructure owners and operators and State, local, tribal, and territorial (SLTT) governments are crucial consumers and providers of risk information. This culture is built on a shared understanding of national and state efforts toward greater critical infrastructure security and resilience⁴.

Collaboratively managing risk requires sharing information (including smart practices), promoting more efficient and effective use of resources, and minimizing duplication of effort. It enables the development and execution of more comprehensive measures to secure against, disrupt, and prepare for threats, mitigate vulnerabilities, and reduce consequences across Wisconsin.

⁴ U.S. Department of Homeland Security (2009) National Infrastructure Protection Plan (NIPP). Washington, DC



Response Plan Annex

Response Plan Annex

Response Annex Introduction

General

1. "Many of the nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent critical infrastructure and key resources (CIKR) and ultimately to our economy and national security." (National Strategy for Homeland Security, October 2007).
2. Personal, public, and private sector business information storage and transfer are common practices in today's world. Information technology devices, including computers, tablets, smart phones, and other such devices, play a critical role in our information driven society. Information exchange via local and wide area networks and the internet, collectively known as 'cyberspace', touches every corner of the planet. The cyber space environment remains vulnerable to threats and attacks by a wide range of nefarious individuals and groups ranging from lone-wolf hackers and criminal enterprises to nation states intent on disrupting our way of life. A credible cyber threat or a cyber incident may affect one or more state agencies, counties, tribes, businesses and critical infrastructure locally, across the entire state, or even the nation.
3. This annex recognizes these vulnerabilities and establishes guidance for state agencies for a coordinated, multidisciplinary, broad-based approach to prepare for, and respond to cyber-threats and incidents.

Purpose

1. This annex:
 - a) Is an element of the Wisconsin Emergency Response Plan, a comprehensive state-level emergency management planning strategy.

- b) Establishes a standardized, flexible, and scalable foundation for state agency preparation for, and response to a threat or attack involving state networks, local government networks, and networks involved in supporting critical infrastructure.
- c) Provides guidance to state agencies regarding mitigation, prevention, protection, and response to actual or potential cyber related threats and attacks.
- d) Provides guidance to counties, tribes, and local units of government regarding available state assets and resources.

Scope


1. This annex:

- a) Describes the framework within which state agencies:
 - (1) Proactively protect and defend state owned data systems and networks.
 - (2) Support local units of government in a cyber related incident as required by §323.01 of the Wisconsin Statutes.
- b) Is not intended to supersede or replace state agency plans and procedures. Users are responsible for being familiar with and implementing their agency's standing plans and procedures.
- c) Recognizes that the whole community shares responsibility for maintaining awareness of and taking action to address risk and reduce vulnerability. For the purposes of this annex, the 'whole community' includes:
 - (1) Individuals and households.
 - (2) Communities (including professional associations) faith-based organizations, neighborhoods, and other such groups.
 - (3) Private sector entities including businesses, industries, schools and universities, and other private enterprises.
 - (4) Non-governmental organizations.
 - (5) Local units of government including municipalities, counties, and tribes.
 - (6) Wisconsin state agencies.
 - (7) Cooperating federal agencies.
- d) Is intended to develop broad concepts focused on Wisconsin's interface with federal agencies including:

- (1) US DHS Office of Cyber Security and Communications including the National Communications System (NCS), the NCS National Coordinating Center (NCC), National Cyber Security Division (NCSD), NCSD United States Computer Emergency Readiness Team (US-CERT), and Office of Emergency Communications (OEC).
- (2) DOD Cyber Crime Center (DC3), US Strategic Command, and the subordinate US Cyber Command
- (3) Federal Bureau of Investigation (FBI).
- (4) US DHS/Secret Service (US SS).

2. For the purposes of this annex:

- a) 'Cyber' refers to the relationship between computer hardware and software including electronic tablets, smartphones, and other similar devices and the interconnections between them for the collection, electronic storage, and dissemination of information.
- b) 'Cyberspace' means the electronic environment for information transfer including public and private local and wide area networks and the internet.
- c) 'Cyber incident' means an occurrence related to computers, servers, controls, electronic files, email systems, software, networks, or the internet requiring a response to protect life, property, the environment, or the economy.
- d) The 'Cyber environment' includes all physical and virtual assets in cyberspace.
- e) 'Cyber threat' means the intent to, or possibility of, a malicious attempt to damage or disrupt computer equipment or networks, or exfiltrate electronic information at rest or in transit for nefarious purposes.
- f) 'Cyber critical infrastructure' means physical or virtual systems and assets vital to Wisconsin which, if incapacitated or destroyed, would have a debilitating impact on Wisconsin's safety, security, economy, public health, or any combination of those matters.
 - (1) The Wisconsin Critical Infrastructure Level 4 List includes facilities identified as cyber-critical infrastructure.
- g) 'Significant Cyber Incident' means an occurrence presenting a set of cyber-related conditions requiring an increased level of scrutiny and potential response.



Training & Exercise Annex

Training & Exercise Annex

Executive Summary

Wisconsin's Cyber Disruption Plan (WCDP) is a capstone document developed under the direction of the State of Wisconsin Chief Information Officer.

Human Capital Development

Operationalization of the WCDP will require a concerted effort to develop and maintain critical human capital assets in an unprecedented period of workforce turbulence.

Homeland Security Exercise and Evaluation Program

The WCDP is the first of the disruption plans to take a holistic, whole community¹, approach to a cyber disruption and follows the Department of Homeland Security Exercise and Evaluation Program.

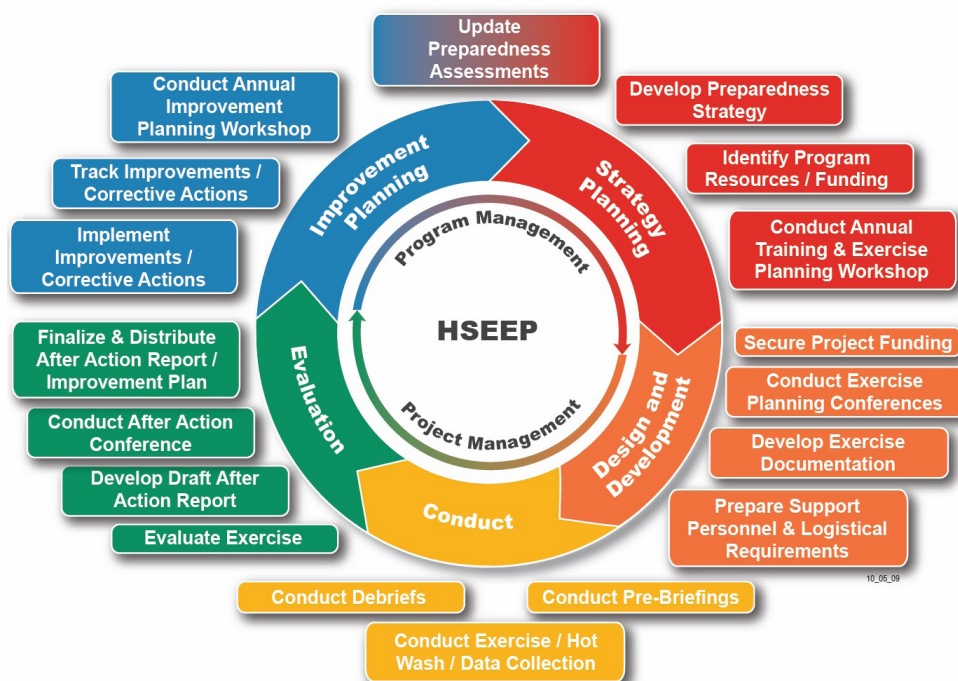


Figure 1: Homeland Security Exercise and Evaluation Program

¹ FEMA. "Whole Community." Undated. Available at: <http://www.fema.gov/whole-community>

At the organizational level this Annex of the WCDDP approach to exercise design follows the Homeland Security Exercise and Evaluation Program.²

“The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Exercises are a key component of national preparedness—they provide elected and appointed officials and stakeholders from across the whole community with the opportunity to shape planning, assess and validate capabilities, and address areas for improvement.”

This Annex does not duplicate HSEEP and should be read in conjunction with the HSEEP.

Strategy and Planning

This Annex supports the identification and development of specific cyber risk profiles in each of the CIKR sectors developed with the initial WCDDP and subsequent revisions. The training and exercise strategy is derived from:

- Identification of risks within the sector of the state government nexus. Importantly the cyber disruption plan is focused on the support CIKR asset owners/operators have identified as being required from governmental agencies.
- CIKR Supported and Supporting Relationships. The exercise strategy recognizes the domino effect of a cascading failure. Training and exercises must fully incorporate elements that reflect the interdependencies of CIKR.

² US DHS. “Homeland Security Exercise and Evaluation Program (HSEEP).” April 2013. Available at: <https://www.fema.gov/media-library/assets/documents/32326>

Design and Development

- **Planning Team Composition.** The members of the planning team should be carefully selected with deep technical skills within their respective organizations and a working understating of exercise development. A lead planner with Master Exercise Practitioner qualifications is critical to maintain doctrinally sound strategy and planning documents.
- **Master Scenario Event List (MSEL) development.** The MSEL is a critical component of a viable exercise. Visible HSA/CIO involvement in CS III is critical to the development of cyber response and recovery expertise. Although the term “Cyber War” was first coined in 1984, incident command is still largely focused on law enforcement, fire, and EMS response protocols for traditional large scale incidents.

Conduct Training and Exercises

- **Federal, State and Local Interagency Coordination.**
- **National Guard Establishment and Wisconsin Statewide Information Center (Fusion Center) participation.**
- **Federal Agency Participation.** This exercise stressed the importance of understanding home rule as well as emergency declarations and powers as it applies to local units of government and their interface with state agencies and private entities.

Evaluate the Results of Training

- State Emergency Operations Center (E-SPONDER®). E-SPONDER® functions and features should be fully exploited in planning and preparing for a cyber incident. Additionally, plans should recognize that E-SPONDER® may not be available as a result of a cyber incident.
- Establishing Response Triggers. Triggers for reporting, implementing an increased level of vigilance, needs to be more clearly defined while establishing the E-SPONDER® site. ICS response to cyber incidents would be dictated by the nature of the incident, regardless of a cyber incident having a causal relationship.
- Standardize and Communicate Alert Level Definitions. It is critical to ensure that those who represent state and local units of government clearly understand relevant alert levels as they are key decision-makers during an incident.
- Public Information Function Needs to be Well Designed. It is important to coordinate the role of public information at the local level and state level to ensure a consistent message to the public.

Human Capital

Introduction

An effective continuous training and learning strategy is a key element of the WCDP. The individual employees with cyber response responsibilities require an investment of time and energy to keep pace with the rapidly changing cyber infrastructure.

This annex includes, by reference, the US Office of Personnel Management's guide to Learning Strategies for Creating a Continuous Learning Environment.³

Malcolm Shepherd Knowles was an American educator well known for the use of the term Andragogy as synonymous to adult education. According to Malcolm Knowles, andragogy is the art and science of adult learning. The investment of time requires the application of adult learning principles. *"Knowles is credited with being a fundamental influence in the development of the Humanist Learning Theory and the use of learner constructed contracts or plans to guide learning experiences."*⁴

The concept of andragogy had been in spasmodic usage since the 1830s, primarily in Germany. It was Malcolm Knowles who popularized its usage for English language reader with five basic assumptions:

- Self-concept: As a person matures his self-concept moves from one of being a dependent personality toward one of being a self-directed human being
- Experience: As a person matures he accumulates a growing reservoir of experience that becomes an increasing resource for learning.

³ US OPM. "Learning Strategies for Creating a Continuous Learning Environment." September 2005. Available at: <https://www.opm.gov/policy-data-oversight/human-capital-management/reference-materials/leadership-knowledge-management/continuouslearning.pdf>

⁴ Smith, Mark K. "Malcolm Knowles, Informal Adult Education, Self-direction and Andragogy". Encyclopedia of Informal Education. Retrieved August 13, 2011.

- Readiness to learn. As a person matures his readiness to learn becomes oriented increasingly to the developmental tasks of his social roles.
- Orientation to learning. As a person matures his time perspective changes from one of postponed application of knowledge to immediacy of application, and accordingly his orientation toward learning shifts from one of subject-centeredness to one of problem centeredness.
- Motivation to learn: As a person matures, the motivation to learn is internal.

Knowles' 4 Principles of Andragogy consist of the following applied concepts to adult learning:

- Adults need to be involved in the planning and evaluation of their instruction.
- Experience (including mistakes) provides the basis for the learning activities.
- Adults are most interested in learning subjects that have immediate relevance and impact to their job or personal life.
- Adult learning is problem-centered rather than content-oriented.

Representatives by CIKR Sectors

Banking and Finance

Associated Bank
Department of Financial Institutions
Johnson Bank

Chemical

Hydrite Chemical

Commercial Facilities

Kohls

Communications

5NINES
AT&T
Public Service Commission

Critical Manufacturing

GE Healthcare

Dams

WI Valley Improvement Company
WPS

Defense Industrial Base

Department of Military Affairs
Oshkosh Defense
FBI

Emergency Services

Darley

Energy

Alliant Energy
Nextera Energy (Point Beach)
Public Service Commission
We Energies
Xcel Energy

Food and Agriculture

Department of Agriculture, Trade and
Consumer Protection
Kwik Trip

Government Facilities

Department of Administration

Healthcare and Public Health

Department of Health Services
University of Wisconsin
UW Health

Information Technology

5NINES
Department of Administration
IBM
New North Venture LLC
University of Wisconsin

Nuclear Reactors, Materials and Waste

Nextera Energy (Point Beach)
Public Service Commission

Transportation Systems

Department of Transportation
Schneider Trucking

Water and Wastewater Systems

Milwaukee Waterworks
Public Service Commission