CHAPTER 3.10
RISK ASSESSMENT: CYBER DISRUPTION

3.10 Risk Assessment: Cyber Disruption

Description

A significant cyber disruption event as defined from the National Cyber Incident Response Plan dated September 2010 as “an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state.”

Cyber disruption is a hazard that touches many aspects of communities: industry, government, health, business, and private. As information technology continues to flourish and grow in capability and interconnectivity, cyber disruptions become increasingly frequent and destructive. They are a fast-growing area of crime and more criminals are using the Internet to commit a diverse range of criminal activities. These types of crimes can cause serious harm and pose a real threat to victims worldwide (INTERPOL 2017).

Cyber security has shifted its focus from preventing initial entry to limiting damage once a system has been penetrated by identifying breaches and isolating the malware to stop it from Centralized systems like Supervisory Control and Data Acquisition (SCADA) are used to control infrastructure such as: communications, utilities, transportation, medical facilities, law enforcement, business, financial systems, and personally identifiable information (PII), all which may be compromised by cyber disruptions spreading. A state cyber-security group is working to address risk to state agencies’ systems.

In 2016, the State of Idaho ranked 40th in the United States for the number of cybercrime victims reported to the Internet Crime Complaint Center. The State ranked 37th for losses per victim as reported to the Internet Crime Complaint Center (Federal Bureau of Investigation 2016).

Currently the state’s executive branch agencies all have internal Information Technology (IT) departments that work and operate independently. House Bill 607 was passed in the 2018 legislative session: “To establish in the Office of the Governor the Office of Information Technology Services. This office will oversee and coordinate implementation of information technology services and cybersecurity policies within the State of Idaho. The existing information technology services functions currently performed by the state's Department of Administration would be transferred to this new office to facilitate consolidation and efficiency of IT service and cyber security efforts across all agencies.” Specific to the cyber disruption hazard, the new agency will be charged:

> (5) To oversee implementation of cybersecurity policies to foster risk and cybersecurity management telecommunications and decision-making with both internal and external organizational stakeholders. (6) To coordinate and consult with state agencies and officials regarding information security needs.

(7) To coordinate with state agencies and officials on penetration tests and vulnerability scans of state technology systems in order to identify steps to mitigate identified risks.

(8) To coordinate with state agencies and officials to ensure that state agencies implement mandatory education and training of state employees and provide guidance on appropriate levels of training for various classifications of state employees.

(9) To coordinate with appropriate state agencies to create, coordinate, publish, routinely update and market a statewide cybersecurity website as an information repository for intelligence sharing and cybersecurity best practices.

(10) To coordinate public and private entities to develop, create and promote statewide public outreach efforts to protect personal information and sensitive data from cyber threats.

(11) To promulgate and adopt reasonable rules for effecting the purposes of this act pursuant to the provisions of chapter 52, title 67, Idaho Code.

Idaho state law requires entities to notify affected individuals of a data breach as soon as possible, unless a “good-faith, reasonable, and prompt” investigation reveals that the personal information has not and will not be misused. This law also applies to businesses that maintain personal data for another entity. Idaho Code 28-51-05, in the Commercial Transactions Code, states “Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity”.

(1) A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho attorney general.

Nothing contained in this section relieves a state agency’s responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the Idaho technology authority policies.

Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars ($2,000), or by imprisonment in the county jail for a period of not more than one (1) year, or both.

(2) An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or

> license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.
> (3) Notice required by this section may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice required by this section must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, individual or commercial entity that notification will no longer impede the investigation.

For the purpose of this SHMP update, the following types of cyber disruptions that may occur in the State to be discussed further are: cybercrime, cyber terrorism, and space weather.

Cybercrime

Computer systems on the county, local, and individual level are likely to experience a variety of cybercrime, from malware to targeted attacks on system capabilities. These cybercrime attacks specifically seek to breach information technology (IT) security measures designed to protect an individual or organization. The initial attack is subsequently followed by further, more severe attacks for the purpose of causing harm or stealing data. Organizations are prone to a multitude of different types of attacks. Table 3.10.A10.A describes the most common types of cyber-attacks seen today.

Table 3.10.A. Common Cyberattack Mechanisms

Type	Description
Social Engineering	In the context of cyber-security, this refers to an effort to psychologically manipulate a person, especially through misrepresentation or deception (as in a con game), to gain access to information. The manipulation often relies on the trusting nature of most individuals, or makes use of many persons' natural reluctance to offend others or appear too mistrustful. The ruse may involve creating impressions that make things appear more benevolent, trustworthy, and reliable than they actually are. Some schemes are very complex, and involve several stages of manipulation over a substantial period of time.
Socially Engineered Trojans	Programs designed to mimic legitimate processes (e.g. updating software, running fake antivirus software) with the end goal of human-interaction caused infection. When the victim runs the fake process, the Trojan is installed on the system.
Unpatched Software	Nearly all software has weak points that may be exploited by malware. Most common software exploitations occur with Java, Adobe Reader, and Adobe Flash. These vulnerabilities are often exploited as small amounts of malicious code are often downloaded via drive-by download.
Spoofing	Attempting to gain access to a system by posing as an authorized user, synonymous with impersonating, masquerading, or mimicking. Attempting to fool a network user into believing that a particular site was reached, when actually the user has been led to access a false site that has been designed to appear authentic, usually for the purpose of gaining valuable information, tricking the user into downloading harmful software, or providing funds to the fraudsters.
Malware	Software that can destroy data, affect computer performance, cause a crash, or even allow spammers to send email through an account.
Phishing	Malicious email messages that ask users to click a link or download a program. Phishing attacks may appear as legitimate emails from trusted third parties.

Type	Description
Spear Phishing	A form of phishing that targets a specific individual, company, or agency, usually relying on an accumulation of information to make subsequent ruses more effective when further probing the target, until a successful security breach finally becomes possible.
Pharming	Arranging for a web's site traffic to be redirected to a different, fraudulent site, either through a vulnerability in an agency's server software or through the use of malware on a user's computer system.
Password Attacks	Third party attempts to crack a user's password and subsequently gain access to a system. Password attacks do not typically require malware, but rather stem from software applications on the attacker's system. These applications may use a variety of methods to gain access, including generating large numbers of generated guesses, or dictionary attacks, in which passwords are systematically tested against all of the words in a dictionary.
Drive-by Downloads	Malware is downloaded unknowingly by the victims when they visit an infected site.
Denial of Service Attacks (DoS)	Attacks that focus on disrupting service to a network in which attackers send high volumes of data until the network becomes overloaded and can no longer function.
Man in the Middle (MITM)	MITM attacks mirror victims and endpoints for online information exchange. In this type of attack, the MITM communicates with the victim who believes is interacting with the legitimate endpoint website. The MITM is also communicating with the actual endpoint website by impersonating the victim. As the process goes through, the MITM obtains entered and received information from both the victim and endpoint.
Malvertising	Malware downloaded to a system when the victim clicks on an affected ad.
Adware	A form of software that displays advertising content in a manner that is potentially unexpected and unwanted by users, which may also include various user-tracking functions (similar to spyware).
Spyware	Software that allows others to gain private information about a user, without that person's knowledge or consent, such as passwords, credit card numbers, social security numbers, or account information.
Advanced Persistent Threat (APT)	An attack in which the attacker gains access to a network and remains undetected. APT attacks are designed to steal data instead of cause damage.
Ransomware	Malware that locks a person's keyboard or computer to prevent them from accessing data until you pay a ransom, usually in Bitcoin. A popular variation of this is ransom cryptware, which corrupts files using a private key that only the attacker possesses.
Virus	A program or code that attaches itself to a legitimate, executable program, and then reproduces itself when that program is run.
Worm	A self contained program (or set of programs) that is able to spread copies of itself to other computer systems, usually through network connections of email attachments.

Cyber disruptions may be driven by criminal motives for profit, extortion, or theft, or as deliberate attacks to destroy, damage, or interfere with infrastructure systems. The assessment for the likelihood of an event involving this tactic is moderate, based on a review of threats and trends related to this type of attack methodology both nationally and at the state level. Intelligence also indicates this methodology has been used in limited attacks and attempted attacks both overseas and within the United States with some level of success as a viable tactic. (State of Idaho THIRA 2012 authored by David Jackson)

Cyber Terrorism

The FBI defines cyber terrorism as the premeditated, politically motivated, attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents. It is a deliberate act of computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or computer system or information. The motive behind such disruptions can be driven by religious, political, or other objectives. Similar to traditional terrorism tactics, cyberterrorism's purpose is to evoke very strong emotional reactions such as anxiety, fear, anger, despair, depression, or even sympathy as a recruitment tool for an organization. However, the mechanism for achieving these goals are through IT and not necessarily a tangible violent or physically disruptive action. The purpose of cyberterrorism can be broken out into three main objectives: organizational, undermining, and destructiveness. Each objective indicates a use of IT for a specific purpose (Kostadinov 2012).

As an organizational objective, cyberterrorism includes specific functions outside of or in addition to a typical cyberattack. Terrorist groups today use the internet on a daily basis. This daily use may include recruitment, training, fundraising, communication, or planning. Organizational cyberterrorism can use platforms such as social media, as a tool to spread a message beyond country borders and instigate physical forms of terrorism. Additionally, organizational goals may use systematic attacks as a tool for training new members of a faction in cyber warfare.

Undermining as an objective seeks to achieve the hindrance of normal functioning computer systems, services, or websites. Such methods include defacing, denying, and exposing information. While undermining tactics are typically used due to high dependence on online structures to support vital operational functions, they typically do not result in grave consequences unless undertaken as part of a larger attack.

Three kinds of undermining attacks that can be conducted on computers include attacks of physical means, electronic means, and attacks using malicious code (Waldron 2011). Specifically, these types of attacks include:

Directing conventional kinetic weapons against computer equipment, a computer facility, or transmission lines to create a physical attack that disrupts the reliability of equipment.

The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse (EMP), can be used to create an electronic attack (EA) directed against computer equipment or data transmissions. By overheating circuitry or jamming communications, an EA disrupts the reliability of equipment and the integrity of data.

Malicious code can be used to create a cyberattack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyberattack can disrupt the reliability of equipment, the integrity of data, and the confidentiality of communications (Wilson 2008).

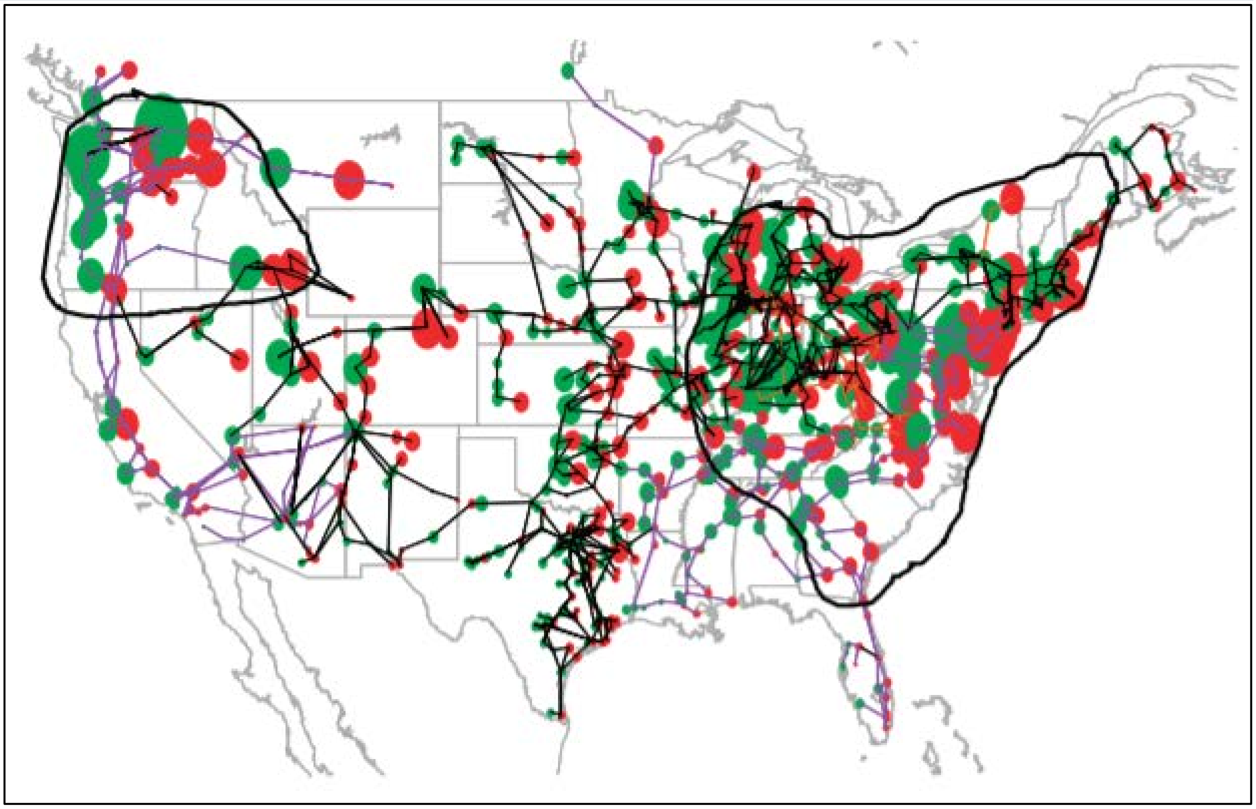
The destructive objective for cyberterrorism is what organizations fear most. Through the use of computer technology and the internet, terrorists seek to inflict destruction or damage on tangible property or assets, and even death or injury to individuals. There are no cases of pure cyberterrorism as of the date of this plan.

Space Weather

Space weather refers to the variable conditions on the sun and in space that can influence the performance of technology used on earth. Extreme space weather could potentially cause damage to critical infrastructure, especially the electric grid. Space weather can produce electromagnetic fields that induce extreme currents in wires, disrupting power lines, and even causing wide-spread blackouts. Severe space weather also produces solar energetic particles, which can damage satellites used for commercial communications, global positioning, intelligence gathering, and weather forecasting. Geomagnetic storms are disturbances in the geomagnetic field caused by gusts in the solar wind that blows by Earth. Solar Radiation Storms are elevated levels of radiation that occur when the numbers of energetic particles increase. Radio Blackouts are disturbances of the ionosphere caused by x-ray emissions from the Sun.

Different types of space weather can affect different technologies on earth. Solar flares can produce strong x-rays that degrade or block high-frequency radio waves used for radio communication during events known as radio blackout storms. Solar Energetic Particles (energetic protons) can penetrate satellite electronics and cause electrical failure. These energetic particles also block radio communications at high latitudes during Solar Radiation Storms. Geomagnetic storms can also modify the signal from radio navigation systems (GPS and GNSS) causing degraded accuracy (Space Weather Prediction Center 2017). Figure 3.10.B below shows regions susceptible to a power grid collapse during a 4800 nT/min geomagnetic field disturbance at 50° geomagnetic latitude, where the densest part of the United States power grid lies. The affected regions are outlined in black. This figure shows that widespread blackouts could occur, impacting more than 130 million people. The entire State of Idaho is shown as being affected in the event of a power outage as a result of this disturbance.

Figure 3.10.B. Regions Susceptible to Power Grid Collapse from a Geomagnetic Storm



Source: *National Research Council 2008*

Note: *Regions susceptible to power grid collapse during a 4800 nT/min geomagnetic field disturbance at 50° geomagnetic latitude, where the densest part of the U.S. power grid lies. The affected regions are outlined in black. Analysis of such an event indicates that widespread blackouts could occur, involving more 130 million people. A disturbance of such magnitude, although rare, is not unprecedented: analysis of the May 1921 storm shows that disturbance levels of ~5000 nT/min were reached during that storm.*

The class of cyber incidents that fit within the term "cyber disruption" can be described through examples such as: (NASCIO, 2016)

- a cyber attack on the power grid leading to loss of power to a significant population;
- a cyber attack on water treatment and delivery leading to a loss of water supply to a significant population;
- cyber attacks on financial management, healthcare providers, transportation systems, education;
- a cyber attack on network capabilities leading to loss of communications which then hampers, interrupts or prevents the operation of government and requires implementation of a Continuity of Operations Plan;
- a hurricane, flood, tornado, earthquake, or other natural disaster that impairs or destroys a key infrastructure asset that then precipitates the loss of connectivity over the internet or internal network;
- natural disaster that impairs or destroys a data center which then precipitates loss of connectivity or loss of data access and requires implementation of a Continuity of Operations Plan;
- a natural disaster that is further complicated due to an ensuing cyber attack; or

- a solar type of event large enough in size to cause some sort of regional cyber disruption.

Location, Extent, and Magnitude

Cyber disruptions are not geography-based; they can occur anywhere across Idaho where technological systems exist or are utilized. They can originate from any computer to affect any other computer in the world. If a system is connected to the Internet or operating on a wireless frequency, it is susceptible. Targets of cyber disruptions can be individual computers, networks, organizations, business sectors, or governments. Financial institutions and retailers are often targeted to extract personal and financial data that can be used to steal money from individuals and banks. The most affected sectors are finance, energy and utilities, and defense and aerospace, as well as communication, retail, and health care. Both public and private operations in the State of Idaho are threatened on a near-daily basis by millions of current cyberattacks developed to automatically seek technological vulnerabilities.

Cyber Crime and Cyber Attack Location, Extent, and Magnitude

It should be noted there is a difference between a cyber incident and cyber disruption. A cyber disruption may initially be identified as a cyber incident depending on the scope. This is also defined by each individual entity depending upon how critical the compromised system or data is.

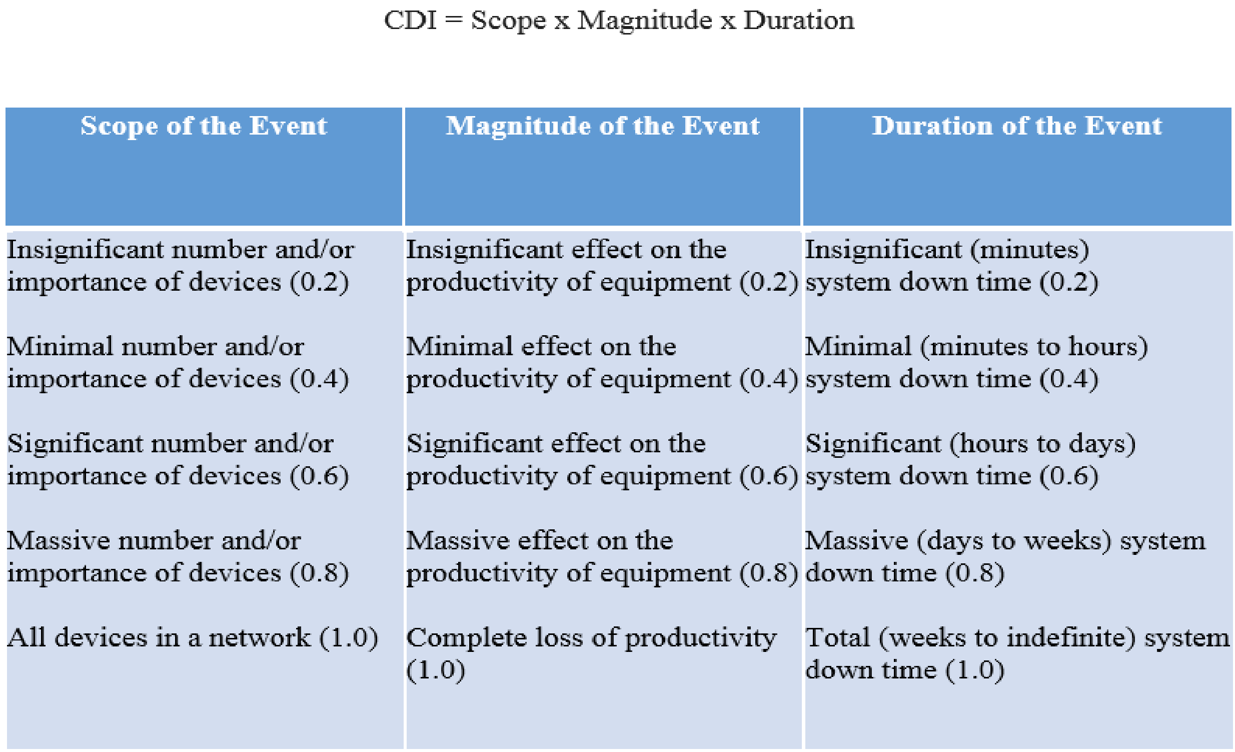
A Cyber Incident would have impacts such as a specific device/system/network; an individual or specific customer base; loss of specific information such as personal identifiable information (PII); limited in time duration (minutes to days); and an objective of containment, restoration, and recovery. (NASCIO, 2017)

A Cyber Disruption would have impacts such as regional, national or multi-national profound detrimental effect on life within a region; impaired or destroyed a critical infrastructure asset such as a data center, power generation plant, distribution of electricity, treatment and distribution of water; and cascade, domino effects of disruptions (e.g., loss of electrical distribution leads to halting of water pumps and thus the distribution of water; without water cooling units in large facilities other equipment fails). Cyber disruptions target a population, a region, a critical infrastructure asset, a certain skill, knowledge, data or information asset

an entire industry or service or service cluster, an entire jurisdiction, a government function, or a government official or role. (NASCIO, 2017).

There is no widely used extent or magnitude ranking for cybercrimes or cyber terrorism at present. The magnitude of extent will vary greatly based on the extent and duration of the impact, and the extent will vary based upon which specific system is affected by an attack, the warning time, and ability to preempt an attack. The Center for International and Security Studies at the University of Maryland developed a Cyber Disruption Index (CDI) with the intent of standardizing assessment of a cyber disruption event for both affected organizations and government officials. The full report and methodology can be found at http://www.cissm.umd.edu/publications/categorizing-and-assessing-severity-disruptive-cyber-incidents. The published study titled Categorizing and Assessing the Severity of Disruptive Cyber Incidents, "compares the consequences of an actual or potential cyber event along three dimensions: scope, magnitude of effect on impacted devices, and duration of the disruption. For mathematical reasons, the value assigned on each dimension needs to be greater than zero and no more than one, so that scores on the three dimensions can be multiplied to get a total CDI value that provides a systematic, if still somewhat subjective, way to compare the overall consequences of different types of attacks against different kinds of organizations. These values can be measured after an event. They can also be roughly estimated for different types of potential attacks by analysts with general knowledge. And they can be calculated more precisely by those who have detailed information about how a particular organization's IT networks and procedures map onto its mission and operations" (CISSM, 2017).

Figure 3.10.C. Cyber Disruptive Index



CDI = Scope x Magnitude x Duration

Scope of the Event	Magnitude of the Event	Duration of the Event
Insignificant number and/or importance of devices (0.2)	Insignificant effect on the productivity of equipment (0.2)	Insignificant (minutes) system down time (0.2)
Minimal number and/or importance of devices (0.4)	Minimal effect on the productivity of equipment (0.4)	Minimal (minutes to hours) system down time (0.4)
Significant number and/or importance of devices (0.6)	Significant effect on the productivity of equipment (0.6)	Significant (hours to days) system down time (0.6)
Massive number and/or importance of devices (0.8)	Massive effect on the productivity of equipment (0.8)	Massive (days to weeks) system down time (0.8)
All devices in a network (1.0)	Complete loss of productivity (1.0)	Total (weeks to indefinite) system down time (1.0)

Source: CISSM 2017

Space Weather Location, Extent, and Magnitude

The NOAA Space Weather Scales were introduced as a way to communicate to the general public the current and future space weather conditions and their possible effects on people and systems. The space weather scales correlate space weather events with their likely effects on technological systems. The scales describe the environmental disturbances for three event types: Geomagnetic Storms (G-scale), Solar Radiation Storms (S-scale), and Radio Blackouts (R-scale). The scales have numbered levels, analogous to hurricanes, tornadoes, and earthquakes that convey severity. The scales also list possible effects at each level, show how often such events occur, and give a measure of the intensity of the physical causes. For details regarding the physical measure and average frequency, refer to the NOAA Space Weather Scales website at: http://www.swpc.noaa.gov/noaa-scales-explanation

Table 3.10.D. Geomagnetic Storms

Scale	Description	Effect
G5	Extreme	**Power systems**: Widespread voltage control problems and protective system problems can occur, some grid systems may experience complete collapse or blackouts. Transformers may experience damage. **Spacecraft operations**: May experience extensive surface charging, problems with orientation, uplink/downlink and tracking satellites. **Other systems**: Pipeline currents can reach hundreds of amps, HF (high frequency) radio propagation may be impossible in many areas for one to two days, satellite navigation may be degraded for days, low-frequency radio navigation can be out for hours, and aurora has been seen as low as Florida and southern Texas (typically 40° geomagnetic lat.).
G4	Severe	**Power systems**: Possible widespread voltage control problems and some protective systems will mistakenly trip out key assets from the grid. **Spacecraft operations**: May experience surface charging and tracking problems, corrections may be needed for orientation problems. **Other systems**: Induced pipeline currents affect preventive measures, HF radio propagation sporadic, satellite navigation degraded for hours, low-frequency radio navigation disrupted, and aurora has been seen as low as Alabama and northern California (typically 45° geomagnetic lat.).
G3	Strong	**Power systems**: Voltage corrections may be required, false alarms triggered on some protection devices. **Spacecraft operations**: Surface charging may occur on satellite components, drag may increase on low-Earth-orbit satellites, and corrections may be needed for orientation problems. **Other systems**: Intermittent satellite navigation and low-frequency radio navigation problems may occur, HF radio may be intermittent, and aurora has been seen as low as Illinois and Oregon (typically 50° geomagnetic lat.).
G2	Moderate	**Power systems**: High-latitude power systems may experience voltage alarms, long-duration storms may cause transformer damage. **Spacecraft operations**: Corrective actions to orientation may be required by ground control; possible changes in drag affect orbit predictions. **Other systems**: HF radio propagation can fade at higher latitudes, and aurora has been seen as low as New York and Idaho (typically 55° geomagnetic lat.).
G1	Minor	**Power systems**: Weak power grid fluctuations can occur. **Spacecraft operations**: Minor impact on satellite operations possible. **Other systems**: Migratory animals are affected at this and higher levels; aurora is commonly visible at high latitudes (northern Michigan and Maine).

Source: Space Weather Prediction Center 2017

Table 1.10.E. Solar Radiation Storms

Scale			Description	Effect
S5			Extreme	**Biological**: Unavoidable high radiation hazard to astronauts on EVA (extra-vehicular activity); passengers and crew in high-flying aircraft at high latitudes may be exposed to radiation risk. **Satellite operations**: Satellites may be rendered useless, memory impacts can cause loss of control, may cause serious noise in image data, star-trackers may be unable to locate sources; permanent damage to solar panels possible. **Other systems**: Complete blackout of HF (high frequency) communications possible through the polar regions, and position errors make navigation operations extremely difficult.
S4			Severe	**Biological**: Unavoidable radiation hazard to astronauts on EVA; passengers and crew in high-flying aircraft at high latitudes may be exposed to radiation risk.

Scale			Description	Effect
				Satellite operations: May experience memory device problems and noise on imaging systems; star-tracker problems may cause orientation problems, and solar panel efficiency can be degraded. **Other systems**: Blackout of HF radio communications through the polar regions and increased navigation errors over several days are likely.
S3			Strong	**Biological**: Radiation hazard avoidance recommended for astronauts on EVA; passengers and crew in high-flying aircraft at high latitudes may be exposed to radiation risk. **Satellite operations**: Single-event upsets, noise in imaging systems, and slight reduction of efficiency in solar panel are likely. **Other systems**: Degraded HF radio propagation through the polar regions and navigation position errors likely.
S2			Moderate	**Biological**: Passengers and crew in high-flying aircraft at high latitudes may be exposed to elevated radiation risk. **Satellite operations**: Infrequent single-event upsets possible. **Other systems**: Small effects on HF propagation through the polar regions and navigation at polar cap locations possibly affected.
S1			Minor	**Biological**: None. **Satellite operations**: None. **Other systems**: Minor impacts on HF radio in the polar regions.

Source: Space Weather Prediction Center 2017

Table 3.10.F. Radio Blackouts

Scale	Description	Effect
R5	Extreme	**HF Radio**: Complete HF (high frequency) radio blackout on the entire sunlit side of the Earth lasting for a number of hours. This results in no HF radio contact with mariners and en route aviators in this sector. **Navigation**: Low-frequency navigation signals used by maritime and general aviation systems experience outages on the sunlit side of the Earth for many hours, causing loss in positioning. Increased satellite navigation errors in positioning for several hours on the sunlit side of Earth, which may spread into the night side.
R4	Severe	**HF Radio**: HF radio communication blackout on most of the sunlit side of Earth for one to two hours. HF radio contact lost during this time. **Navigation**: Outages of low-frequency navigation signals cause increased error in positioning for one to two hours. Minor disruptions of satellite navigation possible on the sunlit side of Earth.
R3	Strong	**HF Radio**: Wide area blackout of HF radio communication, loss of radio contact for about an hour on sunlit side of Earth. **Navigation**: Low-frequency navigation signals degraded for about an hour.
R2	Moderate	**HF Radio**: Limited blackout of HF radio communication on sunlit side, loss of radio contact for tens of minutes. **Navigation**: Degradation of low-frequency navigation signals for tens of minutes.
R1	Minor	**HF Radio**: Weak or minor degradation of HF radio communication on sunlit side, occasional loss of radio contact. **Navigation**: Low-frequency navigation signals degraded for brief intervals.

Source: Space Weather Prediction Center 2017

Severity

“Using the CISSM framework to think more systematically about what could happen in the future suggests many plausible scenarios in which a cyber attack on some part of the critical infrastructure would be a major public concern, and therefore warrants government attention to risk mitigation as well as incident response. Failure to invest in appropriate risk mitigation measures could lead to human deaths, not just economic damage, if a hospital loses access to patients’ electronic medical records in a ransomware attack, or if the equipment control systems of a nuclear power plant or hydro-electric dam were targeted. Electricity or transportation systems for major cities could be shut-down for days, not only by attacks on control systems, but also by other disruptive attacks that public officials may not have even considered. A widespread service disruption lasting hours or days would be bad enough during normal times, but substantially more serious if the city was hosting a global event like the Olympics. Even a sustained Denial of Service attack against a major bank could be a public policy problem if customers lost confidence in the reliability of the banking system" (CISSM, 2017).

A cyber disruption can affect a variety of sectors with potentially severe consequences. The following areas may be affected by an attack:

Health and safety of persons in affected areas: No direct loss of life is expected from an attack. Indirect injuries or deaths may result from secondary effects to critical life-sustaining resources such as energy and water.

Health and safety of response personnel: No direct affects to the health and safety of response personnel are expected; however, critical response systems may be affected.

Continuity of operations: Severe effects to continuity of operations could result if a cyber-attack reached critical operational systems or systems that were needed to carry out the operation.

Property, facilities, and infrastructure: Effects can range from annoyance to complete shutdown of critical infrastructures caused by infiltration of supervisory control and data acquisition (SCADA) systems. Secondary effects could disturb public welfare and property by denying services or providing false readings.

Delivery of services: Cyber-attacks may affect delivery of services if the system was infiltrated and directed to malfunction by self-destructing or overloading.

Environment: Generally, cyber terrorism has no direct effect on the environment; however, the environment may be affected should a release of a hazardous material occur because of critical infrastructure failure.

Economic and financial conditions: Because of the heavy reliance on the electronic transfer of economic and commercial information, the economy could be affected by communication difficulties.

Regulatory and contractual obligations: Cyber-attacks would have no significant effect on regulatory or contractual obligations, other than the possible elimination of electronic records, which would affect both.

Reputation of the entity: If exposed vulnerabilities were known and not reduced or eliminated before the attack, the entity would suffer major damage to their reputation for not taking action before the incident.

Electric power, spacecraft, and aviation industries are the main industries whose operations can be adversely impacted by space weather events. The effects of space weather can also be experienced by the growing number of Global Positioning System (GPS) users, such as the oil and gas industry, which relies on GPS data to support offshore drilling operations. Space weather events can lead to major power outages, which has the potential to affect nearly all sectors of society: communications, transportation, banking and finance, commerce, manufacturing, energy, government, education, health care, public safety, emergency services, food and water supply, and sanitation. The severity of the impacts depends on numerous variables, including the duration of the outage (National Research Council 2009).

Warning Time

A cyber disruption can occur with relatively little or no warning. In 2015, the State of Idaho established the Idaho Cybersecurity Taskforce that implements strategies and processes to detect vulnerabilities, prevent future attacks, and protect state governmental networks (Otter 2015).   At the federal level, numerous agencies (such as Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA)) are working collaboratively to thwart cybercrimes and cyber terrorism attacks. The warning time depends upon the ability of these agencies to recognize that a threat exists and their ability to stop the attack. Even with these agencies on task to monitor cyber threats, a cyber-disruption can occur with no warning.

Relationships to Other Hazards

Secondary Impacts

Cyber disruptions have an almost limitless potential to impact all of the human-caused hazards in both numerous and unforeseen ways. Power grid systems are susceptible to cyberattacks and when impacted, could lead to long-term power outages. It has been noted that malicious software could harm critical infrastructure operations, including power systems.   In regards to natural hazards, while cyber disruptions cannot directly influence those events, it is possible for related systems to be affected. For instance, any computerized systems that manage flood control systems could potentially be impacted by a cyber-event, thereby possibly causing a flood event. Cyber disruptions could impact the environment in a number of ways, as affected systems could to stop functioning as intended. It is difficult to predict such impacts as the systems that could be possibly involved are so numerous and complex.

Cyber disruption could also be caused by several other hazards. Earthquakes, flooding, and extreme weather such as severe storms could cause any number of cyber disruption issues through availability of the cyber network. If hardware, computer systems, networks, servers, and backups are damaged due to other hazards, it will cause a cyber disruption for that specific area damaged.

Past Occurrence

While no major direct cyber disruptions have affected Idaho or its counties, it is a hazard that can impact the State’s computer infrastructure and the services that are provided to the public. Cybercrime and cyber-attack attempts are detected by cybersecurity professionals and thwarted on a daily basis in most areas. Across the United States, concerns over cyber terrorism are growing; former FBI director Louis Freeh warns that cyber-terrorism could have a crippling effect in the United States (ANI 2013).

Cyber-attacks are increasing in size, sophistication and cost. Many of the recent attacks have targeted the energy sector. Cyber theft is the fastest-growing crime in the United States and cost the global economy more than $450 million in 2016 (Summerville 2017). A May 2016 report conducted by the Government Accountability Office (GAO) found that cyberattacks against the U.S. government have increased drastically over the past ten years; rising from 5,500 attacks in 2006 to over 77,000 attacks in 2015 (Zeldin 2016). By 2021, cybercrime damage costs could hit $6 trillion annually (Summerville 2017).

Cyber-attacks have also increased in the banking and finance sectors. Hackers have attacked company computers, distracting employees and interfering with Internet Security Providers (ISP) to divert resources, take proprietary information, and steal PII. Small devices can wreak havoc and disrupt systems. Some USBs have been manufactured with viruses or may become infected and spread viruses to multiple computers. Firewalls, access via signatures, and anti-virus are becoming antiquated security methods. Additionally, solar activity is closely monitored as the sun storms have increased since 2011.

The 1859 Solar Flare is the largest magnetic explosion recorded and is referred to as the Carrington Event, named for British Astronomer Richard Carrington, who witnessed growing sunspots and documented a bright white flash that lasted about five minutes. The impacts on Earth were colorful and bright auroras were seen as far south as Hawaii and Cuba. Telegraph operators experienced sparks from telegraph equipment that started fires. Scientists predict that such an event today would be devastating to the internet, communications, and power transformers, as well as satellites, airplanes, or any GPS guided system. Solar activity is closely monitored as the sun storms have increased since 2011.

FEMA Disaster Declarations

Between 1954 and 2017, FEMA has not included Idaho in any cyber disruption-related disasters (DR) or emergencies (EM) declarations. Generally, these disasters cover a wide region of the State; therefore, they may have impacted many counties. However, not all counties were included in the disaster declarations as determined by FEMA (FEMA 2017).

Future Occurrence

As is the case for any large government organization, the State of Idaho will continue to be impacted and compelled to respond to cyber disruption events in the future. The nature of these attacks is projected to evolve over time. With the establishment of the Idaho Cybersecurity Taskforce in 2015, strategies and processes to detect vulnerabilities, prevent future attacks, and protect state governmental networks are being developed (Otter 2015). Solar storm activity is expected to occur in the future as well. Solar storms will likely cause one or more serious infrastructure failures in the future, due to the extent of reliance on electronic and satellite systems that are vulnerable to disruptions. In the event of solar storms, NASA’s Solar Shield Project shows strong currents and warn power companies to protect their systems.

Environmental Impacts

Cyber disruptions could impact the environment in a number of ways, as affected systems could to stop functioning as intended. It is difficult to predict such impacts as the systems that could be possibly involved are so numerous and complex. For instance, any computerized systems that manage flood control systems could potentially be impacted by a cyber-event, thereby possibly causing a flood event.

Climate Change Impacts

Although cyber disruption is categorized as a human-caused hazard, climate change impacts could have cascading effects potentially causing a cyber disruption. Such instances would be severe storms, as well as flooding associated with potential rain on snow events. If the damage was caused to computer systems or servers, this could cause a cyber disruption for that agency/building.

Development Trend Impacts

An understanding of population and development trends can assist in planning for future development and ensuring that appropriate mitigation, planning, and preparedness measures are in place. The State considered the following factors to examine previous and potential conditions that may affect hazard vulnerability: potential or projected development; projected changes in population; and other identified conditions as relevant and appropriate. The U.S. EPA's Integrated Climate and Land-Use Scenarios (ICLUS) project generated projected population and land use projections for the United States through 2100. The project examined multiple scenarios taking into account various population growth and economic development parameters that have been used as the baseline for the Intergovernmental Panel on Climate Change's (IPCC) Special Report on emissions Scenarios (SRES). Population change took into account assumptions regarding fertility, mortality, and immigration, which was then used to drive the land use projections. Map 2.F. in Chapter 2 (State Profile) displays the projected population growth by 2026. As populations increase, the impacts on a cyber disruption, such as a utility failure, will increase in terms of impacts as more people will be left vulnerable.

Development trends across the State can greatly influence and impact future cyber events. As the state gains more population, the number of connected devices will increase, thus increasing the number of Idaho's citizens potentially impacted.

Vulnerability Assessment

Government and industry have been reluctant to publically report any type of vulnerability information on a large scale. As mentioned in some of the previous sections, some vulnerability assessments have occurred as they relate to very specific systems (i.e. An at-risk transformer capacity in Idaho is estimated at 47%). But no specific, statewide vulnerability assessment yet exists for the hazard of cyber disruption.

Critical Infrastructure and State Facility Impact

Government and industry have been reluctant to report and share information on the cyber disruption hazard to protect public image and suppress the release of information to the attackers. Cyber disruption events with malicious intents are difficult to predict. For space weather-caused cyber disruption events, it may be easier to predict and prepare for a disruption. As described in the hazard profile section, NASA's Solar Shield Project shows strong currents for solar storms and warns power companies to protect their systems. Power companies and other private or government agencies can use these warnings, as well as those from NOAA's Space Weather Scales to prepare for the potential impacts from a cyber-disruption.

Executive Order 13636 states, "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cyber security. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats." The use of classified information will be expanded from defense industries to include critical infrastructure industries "enabling near real-time sharing" to assist in security efforts. (Rockwell, 2013). The rapid growth of social media use and technology has increased the potential of cyber disruption exponentially. The commonplace use of computers in practically every office and system contributes to the complexity of mitigating cyber threats. Government and industry are striving to use continuous monitoring and limiting the data that may be accessed once a system is breached.

Loss Estimation

All State-owned and leased buildings in Idaho are exposed and potentially vulnerable to cyber disruption because of their importance in the daily operation of the State. While the physical structures of these buildings are not vulnerable, the information systems within them are. The vast computer networks present in State-owned and leased buildings contain sensitive data that are integral to the security of Idaho. The average amount of money it takes to recover one record of data is $120, and the average medium size business recovery costs about $50,000.

Similarly, critical facilities are vulnerable to cyber disruption based on the significance of the facilities, and the potential to interrupt critical systems in the State. Many critical facilities are reliant upon computer networks to monitor and control critical functions. A cyber disruption could result in catastrophic failure of one of these facilities. Likewise, the power grid is reliant upon computer systems to distribute power to the State. An attack could disrupt power to millions of residents. These are just two examples of how critical facilities are vulnerable to cyber disruption. Given the importance of critical facilities to daily living activities, these facilities are highly vulnerable to cyber-terrorism attacks.

Assessment of Local Vulnerability and Potential Losses

For the purposes of this plan, the entire population of Idaho is exposed to disruptive cyber-related events. Impacts can range from minor malware incidents to more catastrophic impacts to services and facilities providing critical support to residents. The cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. Cyber-crimes can cause damage to a company's brand and reputation, consumer losses from fraud, the opportunity costs of service disruption and "cleaning up" after cyber incidents, and the cost of increased spending on cybersecurity. McAfee issued a report estimating the global cost of cybercrime could be costing as much as $575 billion annually (Paganini, 2014).

If the attack targets critical infrastructure (such as the power grid) impacting life support systems in a healthcare facility, the effects of a cyber-attack on life, health, and safety could be dire. Likewise, if a cyber-attack affects the emergency response system, such as by rendering the 911 Center or the radio network inoperable, emergency services at the county and local level could be hindered, which may result in increased injury or loss of life during emergency situations. If a cyber-disruption impacts the State's power or utility grid, individuals with medical needs would be impacted the greatest. These populations are most vulnerable because many of the life-saving systems they rely on require power. Power redundancy is recommended for the essential and critical facilities that serve vulnerable populations.

If an attack occurred during months of extreme hot or cold weather, the State's elderly population (those 65 years of age and older) may suffer impacts due to the lack of climate control. Other populations vulnerable to the secondary effects of cyber disruption are young children. If a cyber-disruption targeted a facility storing or manufacturing hazardous materials, individuals living adjacent to these facilities may be vulnerable to the secondary effects, should the attack successfully cause a critical failure at that facility.

Economic impacts of a cyber-disruption could be severe, depending on the nature of the attack itself. Even simple malware that slows the performance of individual computers could result in lost business productivity. Any prolonged period of down time could significantly affect a business's financial performance. Retailers and financial institutions may be targeted to steal personal information so that the attacks' perpetrators can steal money from their victims, such as by opening credit cards with the stolen information.

Vulnerability Summary

Overall, any areas where technological systems exist or are utilized are vulnerable to cyber disruption. Particularly vulnerable is the State capital, the City of Boise, given the concentration of State buildings and the services they provide. As discussed above, the sensitive data housed on the computer networks in State buildings are highly vulnerable to this hazard. State agencies, counties, local governments, and private sector entities will need to perform individual risk and vulnerability assessments for their specific systems and tailor specific plans for each area.

Consequence Analysis Evaluation

On June 8, 2017, a Consequence Analysis Evaluation was conducted aligning with hazards profiled in the State Hazard Mitigation Plan. The assessment was conducted by a diverse planning team comprised of subject matter experts from across the State. This effort mirrored a similar exercise that occurred during both the 2010 and 2013 State Hazard Mitigation Plan updates. The exercise is intended to provide another way to assess the State's vulnerability to its hazards and was conducted as a group exercise. Participants were asked to individually rank the following systems on a scale from 0 (no consequences) to 5 (most severe consequences), separately evaluating both the short-term (0-6 month) and long-term (6+ months) consequences of the scenario.

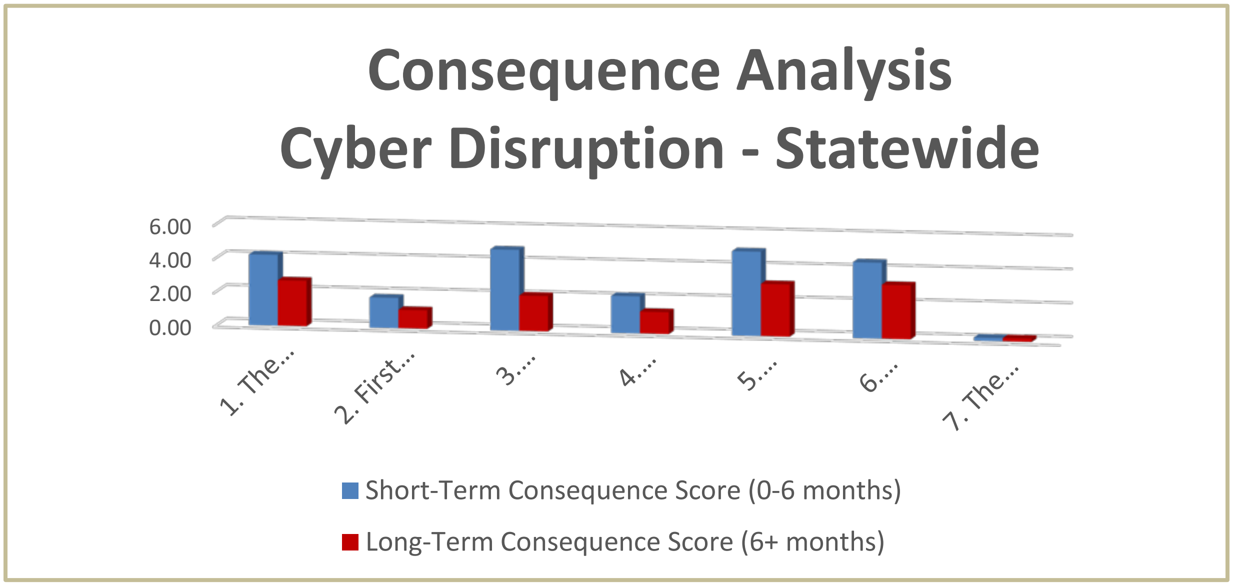
Systems Evaluated:

- The public
- First responders
- Continuity of operations
- Property, facilities, and infrastructure
- Economic conditions
- Public confidence in government

Scenario

October: Over the past several weeks, hackers have conducted cyber-attacks that affect several parts of the nation's financial infrastructure. Specifically, credit-card processing facilities are hacked and numbers are released to the Internet, causing 20 million cards to be cancelled; automated teller machines (ATMs) fail nearly simultaneously across the nation. This week, the Idaho State Controller's Office website has been severely compromised, completely shutting down the system. Today the Idaho Department of Administration website has been hacked as well, causing this website to fail.

Results



Looking at the short-term consequences of this cyber disruption event, exercise participants felt that the most severe consequences would be felt by the economy, continuity of operations, the public's confidence in government, and the public. From a long-term standpoint, the three systems suffering the most severe consequences (in decreasing order) include the public's confidence in government, the economy, and the public. The environment will not be impacted by short or long-term consequences.

Some observations of the group to note included:

- This type of event has the potential to halt both governments and economies.
- This event could easily lead to civil unrest.
- Consequences could quickly escalate to a national and global scale.
- The expected negative consequences are expected to increase in the coming years as our society continues to become more dependent on technology.

Mitigation Rationale

Cyber-attacks across all sectors are growing exponentially. Lessons learned from the most recent ransomware attack on the City of Atlanta prove that this is becoming a larger, fluid threat. "City and government cyber resilience is not aided by the placebo effect that cybersecurity technologies and "safe brands" can create. These blindsides conspire to make the public sector particularly vulnerable to cyber threats. Add in the effect of human errors, indifference and deliberate actions ("between the keyboard and the chair" risks) and hardening the information systems of an entity as complex as a city or [state] comes into focus. All the more so as government transparency, public accountability and digital transformation are highly sought-after goals. The increasing reliance on connected devices to measure everything from traffic flows to water levels and issuing fines through ubiquitous speed cameras, creates an enormous and highly vulnerable attack subsurface. The internet of things (IoT) has opened a veritable Pandora's box of cyber threats that even well-heeled private entities are struggling to contain. [Government entities] will be hard-pressed to get ahead of self-sovereign cyber threats, as well as making the absolute amount of cybersecurity spend a proxy for safety. Many leaders may come to rue the day they connected every citizen service to the internet, without thinking through the potential for unintended consequences" (Disparte, 2018). Due to the universal application of cyber communications, cyber disruptions from natural or human- caused sources will have far reaching impacts.

"Combining city and state requirements to maintain a balanced budget, the measure of economic value at risk together with the reality that taxpayers are the first line of financial defense, makes a compelling case for pooling "blended" risk capital into government cyber risk transfer approaches. Structures that recognize cyber threats (even when monetary demands are relatively small) as potential catastrophic losses can help shield limited public coffers from the economic consequences of these risks. Indeed, Lloyd's research shows that for every 1% increase in insurance penetration, there is a corresponding 22% decrease in the share of risk borne by taxpayers. Cyber risks unlike property damage, which tends to be a finite and easily calculated economic exposure, can cause incalculable harm. Therefore, when it comes to cyber threats, prevention is much better than cure. In short, even if you are fully insured, a cyber threat will be painful" (Disparte, 2018).

"Cities and indeed countries, must consider creating cyber fire brigades as a common good and not as a service spared for those who pay the most money. Cyber threats exploit weak links to get at more desirable or lucrative targets. Therefore, approaches that view cyber threats from the lens of collective defense can go a long way in improving overall resilience. Atlanta's ransomware woes should serve as a wakeup call to all cities and government entities that cyber threats have not only come of age, the next time around the motive may not be monetary. Mercifully Atlanta's cyber-attack had a financial motive and or a path to negotiation. Similar exploits aimed at proving a political point or sowing panic, such as cyber terrorism or an act of cyber warfare, are much harder to respond to and recover from. This highlights the reality that cyber risk is more of a continuity of government threat than a matter of privacy and the provision of basic citizen services" (Disparte, 2018).

Mitigation Strategies for cyber disruption correlate directly with cyber security goals. When considering threats and vulnerabilities, the areas that need to be addressed fall under the umbrella of Access Control. Access control is what will determine the mitigation of the cyber disruption hazard. Access control can be divided into three categories to protect information:

- Confidentiality of Information
- Integrity of Information
- Availability of Information

General Mitigation Approaches

Constant vigilance is required to limit cyber-attacks and automated monitoring is replacing former methods. Information sharing is encouraged to mitigate the spread of known cyber-attacks despite the possibility of making attackers aware of vulnerabilities. It is vital to implement and maintain processes to verify identity and authorize, grant, or deny access to specific locations, information, and networks. Development of risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cyber security initiatives and efforts is recommended. Other approaches could include updating procedures to detect malicious activity and to conduct technical and investigative-based countermeasures, mitigations, and operations. Efforts to coordinate cyber incident management and reporting capabilities are also an action to be considered to help mitigate this hazard. Overall mitigation approaches may include:

- Security appliances and applications
- Backup & restore
- Encryption capabilities
- Authentication, Access, and Accounting (AAA)
- Redundant equipment & networks
- Alternate delivery methods
- Cyber security training and exercises
- Educate public, state employees, and officials
- Contingency planning
- ISP and web hosting reviews
- Share malware signatures
- Coordinate automated responses
- Map suspicious activities
- Anticipate attacks

Cyber Security Policy

In order to mitigate cyber disruption risks, a strong cyber security policy must exist. The security policy should address the following, where applicable: (NRECA, 2011)

- Policy management
- Purpose, scope, and applicability
- Roles and responsibilities
- Implementation and enforcement procedures
- Exceptions
- Policy reviews, approvals, and change management
- Personnel and training
- Personnel risk assessment
- Security awareness program
- Cyber security training
- Critical asset management
- Methodology for identifying critical cyber assets
- Inventory and classification of cyber assets
- Information protection and data privacy

- Cyber vulnerability assessment
- Access control, monitoring, and logging
- Disposal or redeployment of assets
- Maintenance and change control of the asset inventory and classifications
- Electronic security perimeter (ESP)
- Critical assets within the perimeter
- Cyber vulnerability assessment
- Access control, monitoring, and logging
- Configuration, maintenance, and testing
- Documentation maintenance to support compliance
- Physical security
- Critical assets within the perimeter
- Access control, monitoring, and logging
- Incident reporting and response
- Disaster recovery and business continuity plans

The security policy document may address some topics briefly and reference lower-level security policy documents, such as the following: human resources security policy and procedures; guidelines for handling sensitive information assets; physical security policy and procedures; disaster recovery and business continuity plans and procedures; asset disposal procedures; encryption standard and usage guidelines; third-party software and service provider standards; configuration standards; and data backup standard. An additional item to consider within cyber policy is emphasis on a robust security stance that incorporates process controls such as purchasing and acquisition of assets that will have any type of cyber interface through the information technology department, creating a risk profile for vendors, and specific systems security standards prior to purchase.

Hazard Management

In order to reduce the risk of cyber disruption it is important to manage vulnerability, have established backup systems, incident response plans and exercises, disaster recovery, and continuity of operations.

Vulnerability Management: In order to manage the vulnerability, the critical processes required to be operational need to be defined and prioritized. Once this is complete a hardware inventory can help with the vulnerability assessment of an organization. Conduct single points of failure assessments, and identify critical systems and priorities. Systems then need to be defined into terms of high risk systems vs. low risk systems. Critical asset identification and classification can help with this. “Systems have access to and operate using assets that adversaries may want to compromise. Using a risk-based methodology to identify critical cyber assets is a crucial step in managing security risk.

> **Critical assets**: Facilities, systems, and equipment that if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the bulk electric system.
>
> **Cyber assets**: Programmable electronic devices and communications networks including hardware, software, and data.
>
> **Critical cyber assets**: Cyber assets essential to the reliable operation of critical assets.

Note: Risk assessments generally consider both the impact of an adverse event and the likelihood that the event will occur. However, the identification of critical assets considers only the impact of the event; it assumes that the loss will in fact occur" (NRECA, 2011).

Backup Systems: In order to protect against cyber disruption and guard the availability of information, building and maintaining good backup systems and backup power sources is important. Performing regular and scheduled backups can ensure that critical data will still be available after an attack, and can also help make the recovery and restoration process quicker and easier. Offline backups should also be maintained and tested in the event an online system is compromised.

Incident Response: Response to a cyber disruption cannot be ad hoc or made up on the spot. It has to be documented, tested, and implemented. Exercises must be created and held in order to test and refine the incident response plan. Failure to have an implemented incident response will cause a failure in continuity of operations.

Disaster Recovery and Continuity of Operations Plans: Disaster recovery and Continuity of Operations planning is vitally important in the cyber disruption realm in order to mitigate the adverse effects of a disruption. With the increase of cyber disruptions seen across all sectors, it's not a matter of if, but when a cyber disruption, particularly, cyber attack or crime, occurs. The day-to-day operations will most certainly be impacted by these. Practicing the manual processes needed in the event that online systems go down is a critical component to mitigating the effects.

Threat Intelligence

Cyber adversaries are growing in number as well as in sophistication. Leveraging technology and Information shared across multiple entities can assist in understanding the emerging threats as they are detected and understood.

Multi-State Information Sharing and Analysis Center (MS-ISAC). The MS-ISAC is a division of the Center for Internet Security, is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local territory and tribal (SLTT) governments. The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, territory and tribal governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure and two-way sharing of information between and among public and private sectors in order to identify, protect, detect, respond and recover from attacks on public and private critical Infrastructure (CI). The MS-ISAC's 24-hour watch and warning center provides real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the nation's SLTT government cyber domain. (MS-ISAC, 2015). The State of Idaho Information Technology Services (ITS), formerly the Chief Information Office (CIO) in the Department of Administration, is an active member of MS-ISAC and keeps up to date on the latest threats and strategies.

A small number of experts "qualified to protect the nation's infrastructure from a concerted cyber-attack" are hosted by the **Idaho National Labs**, which is a Department of Energy nuclear research and development facility. (Top U.S. Cyber Defenders Work in Idaho Falls, 2012)

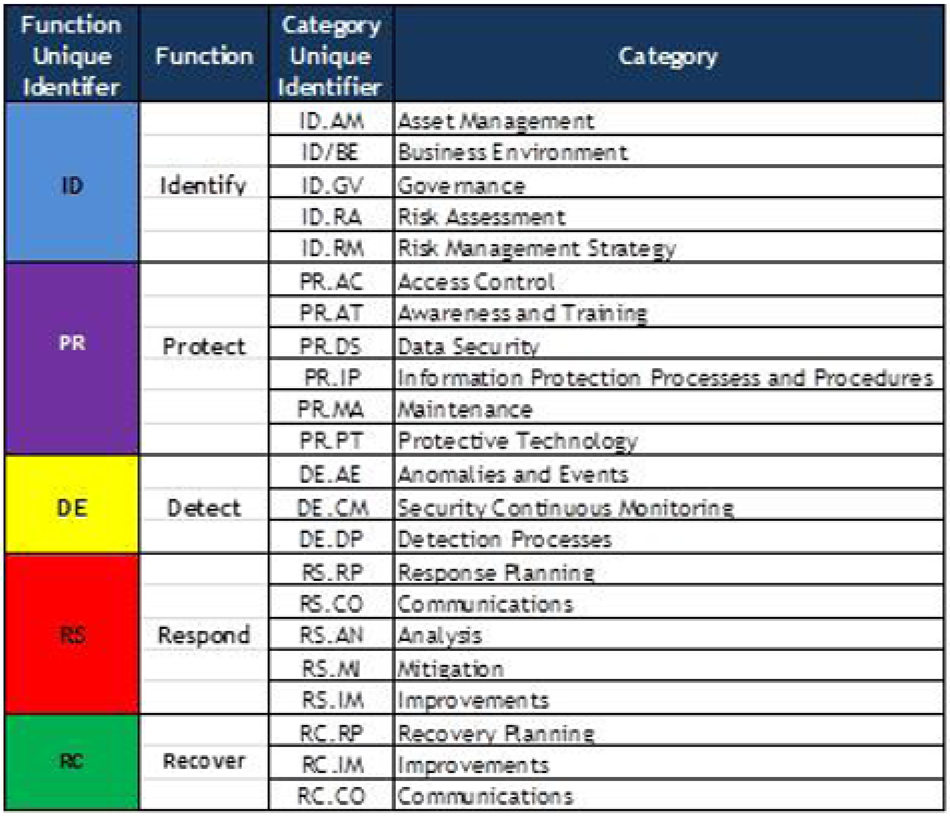
A national organization, **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**, reaches out to assist the technology community. The team is composed of experts who often provide on-site support to organizations, publications, and mitigation briefings.

Staying up to date on current cyber adversary tactics, techniques, and procedures, as well as emerging threats also aids organizations to better be able to conduct cyber kill chain analysis and penetration testing and training specifically for cyber security mitigation. The kill chain was originally used as a military concept related to the structure of an attack consisting of target identification, dispatching a force to that particular target, deciding to attack the target, and then acting upon that target. Lockheed Martin adapted this concept to information security, using it as a method for modeling intrusions on a computer network. (Mason, 2014). Information systems security professionals in an organization can use this type of threat hunting and attack cycle intelligence to mitigate a cyber attack. Penetration testing is a controlled, known targeted attack from a neutral party to evaluate an organization's defense mechanisms. This can include evaluating cyber security policies as well as end-user training for phishing, spear phishing, or whaling. Penetration testing is a key tool for mitigating cyber disruption in the form of cyber attack and crime.

Security Controls

In response to the rapidly changing threat landscape, the critical dependency of information technology in support of virtually all aspects of life, the economy, government, infrastructure and the ability of the nation to respond to emergencies, and in fact the national and economic security of the United States, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. That order directed the National Institute of Science and Technology (NIST) to work with various stakeholders to develop a voluntary framework for cybersecurity that is based on existing standards, guidelines, and practices, and with the purpose of reducing cyber risks to critical infrastructure. (NASCIO, 2016). **The National Institute of Standards and Technology (NIST) Controls.** (NIST, 2013), NIST SP 800-53, provide a catalog of tailorable security controls organized into eighteen families. Each control has zero or more control enhancements which corresponds to the level of impact determined for each control. The level of impact determined adds additional functionality (or enhancements) to increase the strength of the control. The catalog specifies three control baselines: for low, moderate, and high impact information systems. It is recommended to perform a risk assessment first and then select the controls based on the impact level determined as suggested in NIST SP 800-37. Figure 3.10.G below shows the overview of the NIST controls for each function and risk category.

Figure 3.10.G. NIST Controls



Function Unique Identifer	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID/BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processess and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: https://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf

National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems (ICS).

NCCIC ICS works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, NCCIC collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. The ICS-CERT team monitors vulnerabilities to critical infrastructure, responds to intrusions, raises awareness levels, and addresses the need for assessing risk through the Common Vulnerability Scoring System (CVSS). "The CVSS score is an indicator of the severity ranging from 0, meaning no vulnerability present, up to 10, which indicates the highest severity vulnerability. ICS-CERT provides the base CVSS score in advisories as an indicator to asset owners and operators of the severity of the vulnerability. By providing the base metric, readers can use the base metric as a tool to quickly determine the seriousness of the vulnerability associated with the affected system" and "to aid them in prioritizing their mitigation strategies." (ICS-CERT Monitor, 2012) ICS-CERT briefs critical infrastructure owners and stakeholders on threats, security measures, and mitigation actions to reduce risk.

Patch Management. A patch is a small piece of software that a company issues whenever a security flaw is uncovered. The patch essentially covers the hole, keeping cyber adversaries from further exploiting the flaw.

Keeping patches up to date is a best practice in mitigating against cyber disruption, and patch management is an important part of an organization's mitigation arsenal. Many cyber attacks are from the failure to patch quickly enough, or from simply failing to perform the patch. Patch management policy should include timeframes on how often the entity patches, as well as controls to ensure the proper monitoring or assurance system are in place.

Training and Exercises

Among best practices in mitigating cyber attacks and crime for any entity is training of end users. Education of threats and tailored training for employees at each level of access is a measure that will reduce the threat.

Internal Employee Training. Beginning in early 2018, the ITS began implementing state wide training requirements for those with network access. In order to defend the state network against cybercrime, Executive Order 2017-02 was issued, and all state employees are required to complete an annual cybersecurity awareness training campaign. The initial stages contain a four-module campaign that takes approximately 45 minutes to complete.

Email Spoofing. The 5-minute micro-module covers the very important topic of email spoofing. It defines social engineering and shows how hackers can infiltrate an organization and create spoofed emails that trick unsuspecting employees. It also covers a real-life example of just how dangerous email spoofing can be.

Creating Strong Passwords. The 10-minute module covers 10 important rules for creating strong passwords. Users test their own password to see how strong it is, and learn about the latest trend in password security, the passphrase and how to create one.

Ransomware. The fun and engaging course shows users what ransomware is, how it works, and how to steer clear of potential threats. They will meet Sergeant Vasquez, head of our cyber security task force as he takes users through a line-up of the top attack vectors that bad guys use to hold computer systems hostage until a ransom is paid.

Mobile Device Security.

Hackers want to use mobile devices as a gateway to the organization's data. The interactive module puts the power in employee's hands to protect that data. Users will learn about the dangers surrounding Bluetooth, Wi-Fi, apps, and even human error. Users will also learn how to protect the organization from these threats, and then apply this knowledge in three real-life scenarios.

Incident Response and Targeted Threat Training. Going forward, the ITS in conjunction with IOEM, is working to integrate incident response training as a standardized model throughout state agencies. This standardized response will include training on what constitutes an incident, what needs to be reported, and incorporating end user training into the model. Tabletop exercises will be designed to test the training. The ITS is working towards a future training exercise where they are able to conduct a phishing campaign to test end user awareness training for state employees.

Cyber Range. The National Information Assurance Training and Education Center, NIATEC, is consortium of academic, industry, and government organizations to improve the awareness, training and education standards in Information Assurance. It is the federally designated cornerstone for essential education and training components of a strong Information Assurance initiative. The center develops components of effective Information Assurance infrastructure for academic, industrial and governmental organizations.

The NIATEC is associated with Idaho State University Center of Academic Excellence, and both are components of a plan to establish a federal cyber-corps to defend against cyber-based disruption and attacks. The national plan proposed in January 2000 to address the increasing vulnerability to such attacks, emphasizes the role of academia in cyber-defense and calls for active partnerships among private sector, academia, and governmental organizations. Key to building such a cyber-corps is the implementation of robust graduate and undergraduate curricula in Information Assurance. The Director of NIATEC is Dr. Corey D. Schou of Idaho State University. The NIATEC operates as a cyber range which systems can be tested in a controlled environment, much like a simulator, for patch administration as well as penetration testing and cyber security development. This is useful in identifying and testing interdependencies, and serves as a mitigation tool for the shared hazard across all sectors.

Assessment

A future goal of the partnership between ITS and IOEM is to create a self-assessment tool for agencies to be able to conduct internal risk and vulnerability assessments. This will enable to agencies to then be able to implement cyber security strategies specific to that identified risk. This will serve to bridge the gap until the Office of Technology Services is through the transformation strategy and fully has control of the standardized, statewide network control and security. The self-assessment tool will be housed on the ITS website and can also be utilized by the county, city, tribal, and private sectors as well.

Education and Outreach

Public education is important regarding the cyber disruption hazard. As new cybercrime and cyber attack adversary tactics emerge, it is important to ensure that the information is disseminated out to the furthest extent possible.

Web Resources. The ITS has created a website dedicated to public education and outreach, to include publishing newsletters with tips and information. https://cybersecurity.idaho.gov.

Additional online education and outreach resources are:

- Information Systems Security Certifications Consortium, Inc. (ISC) ²." (ISC) ² is an international, nonprofit membership association for information security leaders who are committed to helping members learn, grow, and thrive. (ISC) ² is more than 130,000 certified members strong, and empowers professionals who touch every aspect of information security. More information can be found at https://www.isc2.org.
- The Center for Cyber Safety and Education, a website for cyber education and digital citizenship sponsored by International Information Systems Security Certifications Consortium, Inc. "(ISC) ²." The Safe and Secure Online program offers resources for educators, leaders, and volunteers everywhere to teach the community cyber safety and can be found at https://safeandsecureonline.org.
- The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and

school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. NSCA's website is https://staysafeonline.org.

Learning Events. The Idaho Technology Council (ITC) unifies diverse corporate interests with state and federal government interests. ITC unifies them into a potent value proposition for all by building a competitive work force, driving research out of the lab and into companies, and providing a powerful venue for expanding networks. ITC co-hosts monthly Spark Lunch and Learn series that provide lunch networking opportunities with valuable information security topics to educate those interested in mitigating those risks.

Cyber Security Outreach and Advocacy. The Idaho Department of Labor's Flyer on cybersecurity workforce planning suggests several outreach activities such as apprenticeships, investing in employees, and changing the way most entities think about information technology jobs and the workforce. Additionally, there are recommendations to support education as well as actively advocate for cyber security through establishing relationships with cyber organizations in order to create professional development and training opportunities. Education support includes hosting an in person or virtual field trip for students to learn about the field, or hosting a cybersecurity competition.

Cyber Workforce Generation and Talent Development

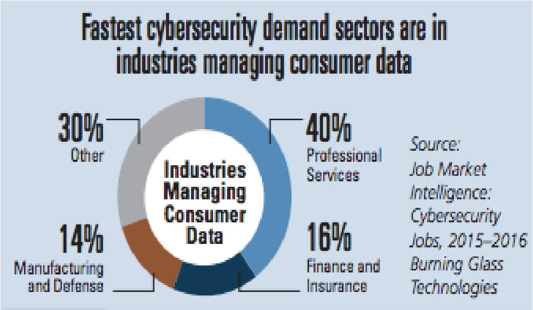
Talent Development and Talent Pipeline. Idaho Digital Learning was created by the Idaho State Legislature (Title 33, Chapter 55 Idaho Statue, 2002) and Idaho educators, developed for Idaho students, and is recognized as a leader across the nation in online virtual education. Idaho Digital Learning was created to provide access, equity, and flexibility for students in the state of Idaho according to its statutory authority, and Idaho Digital Learning enables the state to meet its constitutional requirement to provide a uniform and thorough educational system. The Idaho Technology Council has partnered with the Ms. Greyhat Organization and Idaho Digital Learning to advocate for cyber workforce generation and talent development across the State in order to ensure viable candidates across the public and private sector to work in the cyber security and information technology fields within the state. The partnership is also focused on **Curriculum Development** for kindergarten through high school age children to begin cultivating an awareness and passion for cyber careers.

Apprenticeship. Apprenticeship Idaho, a program within the Idaho Department of Labor, partners with the Idaho Technology Council to develop registered apprenticeships across the state in hard-to-fill cyber security occupations. A Registered Apprenticeship is a combination of relevant training and on-the-job training under the supervision of an experienced mentor. Apprentices receive increases in wages as he/she gains higher skill level and receives a credential/certificate at conclusion. Apprenticeship Idaho is fully funded by a $1.4 million grant from the U.S. Department of Labor to expand registered apprenticeships throughout the state in health care, information technology, advanced manufacturing and energy. Figure 3.10.H. below outlines the Idaho apprenticeship model.

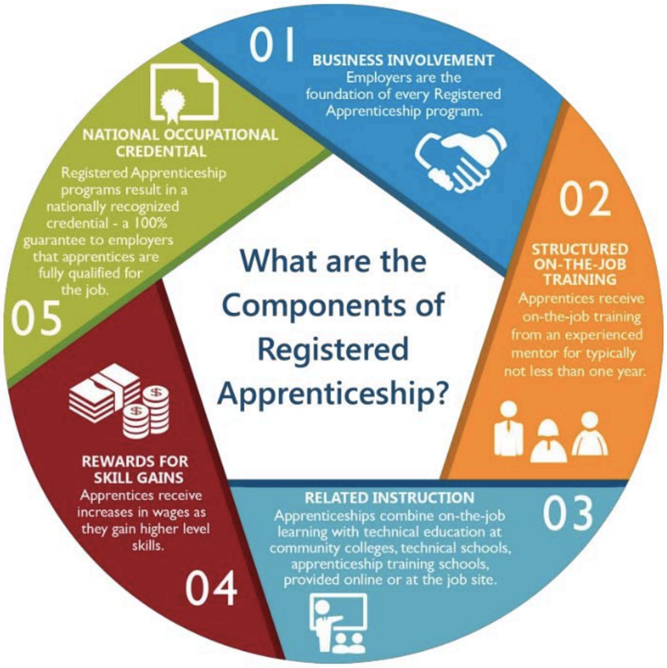
Figure 3.10.H. Idaho Apprenticeship Model

Building Skills. Building the Pipeline. The Registered Apprenticeship model allows employers to take charge of building their own pipeline of highly skilled and highly motivated information security professionals.

Structured, sustainable training that combines learning with doing. Train new workers in cyber security or upgrade the skills of your current workforce with customized, flexible training.



Source: Job Market Intelligence: Cybersecurity Jobs, 2015–2016 Burning Glass Technologies


01
BUSINESS INVOLVEMENT
Employers are the foundation of every Registered Apprenticeship program.
02
STRUCTURED ON-THE-JOB TRAINING
Apprentices receive on-the-job training from an experienced mentor for typically not less than one year.
03
RELATED INSTRUCTION
Apprenticeships combine on-the-job learning with technical education at community colleges, technical schools, apprenticeship training schools, provided online or at the job site.
04
REWARDS FOR SKILL GAINS
Apprentices receive increases in wages as they gain higher level skills.
05
NATIONAL OCCUPATIONAL CREDENTIAL
Registered Apprenticeship programs result in a nationally recognized credential - a 100% guarantee to employers that apprentices are fully qualified for the job.
What are the Components of Registered Apprenticeship?

Your workers also benefit.

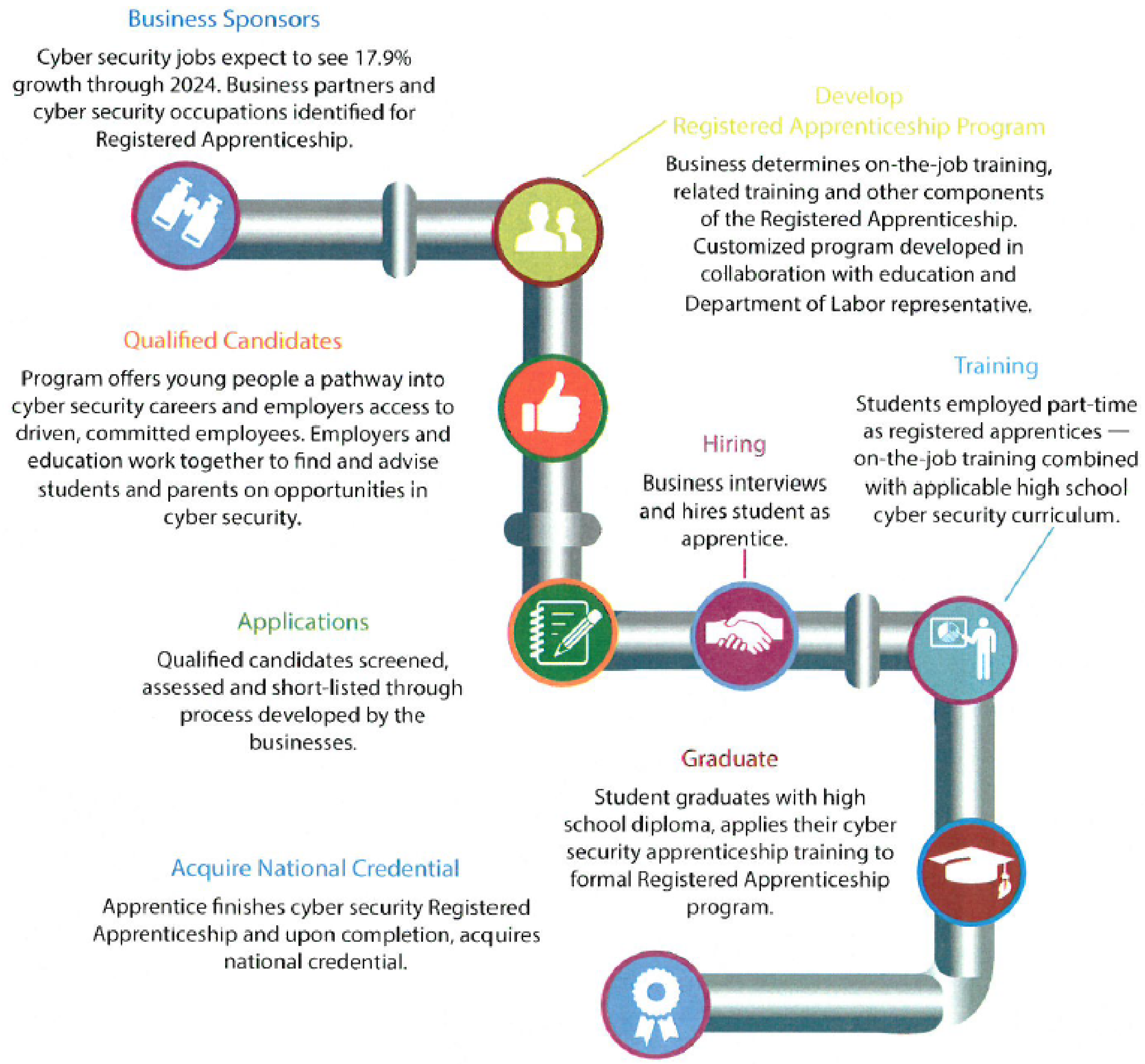
Apprentices receive a paycheck from day one that is guaranteed to increase as their training, knowledge and skills progress – rewarding high-performing employees and moving them up the career ladder in your business.

Productive from day one and more likely to stay on the job.

As employees retire, are promoted or reassigned, you'll be creating career paths for the next generation of skilled workers. You'll also see the impact where it matters most... your bottom line: higher productivity, lower turnover, less recruitment costs and increased workplace safety.

Source: apprenticeshipidaho.com

Figure 3.10.I. Idaho Apprenticeship Model, Continued



Business Sponsors

Cyber security jobs expect to see 17.9% growth through 2024. Business partners and cyber security occupations identified for Registered Apprenticeship.

Develop Registered Apprenticeship Program

Business determines on-the-job training, related training and other components of the Registered Apprenticeship. Customized program developed in collaboration with education and Department of Labor representative.

Qualified Candidates

Program offers young people a pathway into cyber security careers and employers access to driven, committed employees. Employers and education work together to find and advise students and parents on opportunities in cyber security.

Applications

Qualified candidates screened, assessed and short-listed through process developed by the businesses.

Hiring

Business interviews and hires student as apprentice.

Training

Students employed part-time as registered apprentices — on-the-job training combined with applicable high school cyber security curriculum.

Graduate

Student graduates with high school diploma, applies their cyber security apprenticeship training to formal Registered Apprenticeship program.

Acquire National Credential

Apprentice finishes cyber security Registered Apprenticeship and upon completion, acquires national credential.

Source: apprenticeshipidaho.com

Public / Private Partnerships

Cyber disruption is a hazard that cannot be prevented, however, risks can be lowered through mitigation strategies aligned with cyber security to reduce the vulnerability to a disruption as well as increase the resiliency afterwards. Partnerships across the various sectors are key to developing a strengthened and united front to protect against the hazard. **Center for Regional Disaster Resilience**. In 2014, the Idaho Office of Emergency Management and the Pacific Northwest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR) formed a partnership in order to advance cross-sector initiatives that facilitate public-private, cross jurisdictional, regional efforts to develop a disaster resilient state and

region. In the face of emerging risks to economic and national security, action is needed to address crucial regional infrastructure interdependencies in energy, telecommunications, transportation, water systems and other infrastructures. Since 2004, PNWER has hosted numerous exercises focused on cyber security interdependencies to encourage the development of public-private cyber partnerships. (CRDR, 2018).
Cyber Incident Response Coalition and Analysis Sharing (CIRCAS). This organization, including participants from public and private sectors, federal, state, local and tribal government and DHS, academia and law enforcement, was created to share information and resources before, during and after a cyber event. Currently CIRCAS is a Seattle based organization working through the Pacific Northwest National Laboratory (PNNL), however, building this same type of partnership and organization in Idaho will be a key next step in further mitigating the cyber disruption hazard.

Additional Approaches

- Work with insurance companies and risk pools
- Understand the role of the National Guard Cyber Operations Squadron, integrate planning and response efforts
- Foster partnerships with the State Fusion Center for planning and response
- Conduct continued outreach to the Private Sector
- Improve information sharing and situational awareness

THIS PAGE INTENTIONALLY LEFT BLANK