State of Iowa Cybersecurity Strategy

July 2016

Background:

On December 21, 2015, Governor Branstad issued Executive Order 87 (EO87); a cybersecurity initiative for the State of Iowa. The executive order establishes a multi-agency partnership, the EO87 Leadership Team, with the Office of the Chief Information Officer, Iowa National Guard, Department of Public Safety, Iowa Communications Network, and the Iowa Homeland Security and Emergency Management Department. The order directs these agencies to develop a comprehensive cybersecurity strategy which addresses lifeline critical infrastructure, risk assessments, best practices, awareness training, public education and communication, collaboration, K-12 and higher education, data breach notifications, and incident response planning to protect the citizens of Iowa and Iowa businesses.

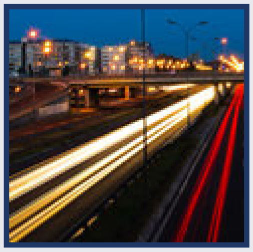
The EO87 Leadership Team, along with several key partners, worked diligently over the last six months to prepare recommendations that will have a direct and sustainable impact on protecting lifeline critical infrastructure, reducing risk to government operations, and creating sustainable partnerships in cybersecurity.

Scope of the Strategy:

The strategy includes a brief description of each executive order element, background information, current state, and recommendations for improving our current state. The primary focus of the strategy is lifeline critical infrastructure sectors (Communication, Energy, Transportation, and Water & Wastewater) and state government as it relates to the protection of citizens and digital government services.

> ***"I, Terry E. Branstad, Governor of the State of Iowa, declare cybersecurity a top priority for this administration and the State of Iowa should protect its citizens and economy against cyberattacks."*** [1]

The strategy does not include detailed operational plans. At the direction of the Governor's Office and Iowa Legislature, the EO87 Leadership Team will prepare an operational plan, budget, and timelines based on the accepted recommendations.



"The bad news is that data breaches are becoming ever more common. The worse news is that the cost they represent for companies is going through the roof.

Those are two conclusions from a study released Wednesday by IBM Security and the Ponemon Institute, which found that the average cost of a data breach has grown to $4 million. That's a hefty jump compared with last year's $3.79 million, and it represents an increase of almost 30 percent since 2013. This year's data uncovered a 64 percent increase in reported security incidents between 2014 and 2015. Meanwhile, the study found that companies now lose some $158 per compromised record. In highly regulated industries like healthcare, the damage is even worse, reaching $355 per record."[2]

Preface: Executive Summary

Overall Management and Sustainability Recommendations:

1. Direct the Office of the Chief Information Officer to formalize and chair the ongoing partnership, collaboration, and structure with the Iowa National Guard, Iowa Homeland Security and Emergency Management Department, Iowa Communications Network, Office of the Chief Information Officer, the Department of Public Safety and other key partners as deemed appropriate by the chair;

    a. Manage all cybersecurity functions as a centralized and accountable state program.
    b. Sustain mutual support and collaboration with industry and federal partners.
    c. Monitor Executive Branch cybersecurity threat and mitigation efforts.
    d. Conduct regular internal and external cybersecurity tests and exercises.
    e. Develop budgetary and other Executive and Legislative support requests.
    f. Report to the Governor and Legislature on strategy progress annually.
    g. Update this strategy every two years.

Specific and Individual Recommendations:

2. Implement the following recommendations detailed in this report;

    a. Implement the National Cybersecurity Framework.
    b. Formalize the Iowa Cybersecurity Incident Response Plan.
    c. Refine the risk assessment process and report on cybersecurity risks within state government and lifeline critical infrastructure.
    d. Consolidate duplicative security products, processes and resources.
    e. Require cybersecurity awareness training, measure effectiveness and report progress.
    f. Institute a public cybersecurity awareness campaign.
    g. Conduct joint training and exercises within state government and with private sector partners identified in Iowa Cyber Incident Response Plan.
    h. Develop STEM scholarships and support structures for the cybersecurity workforce.
    i. Introduce required changes to the Iowa Data Breach notification law.
    j. Incorporate an incident response structure and plan for significant cyber events.

By implementing the recommendations in this report, Iowa will be better able to respond to cybersecurity events, and in-fact proactively mitigate risks for its citizens and government operations.

Combining the accountability of an annual report that includes summarizing risks, priorities, financial and budgetary items, issues, status of initiatives, along with formalizing the EO87 Leadership Team, improves the coordination and increases effectiveness of the state's incident response to cybersecurity events.

Respectively and collectively submitted,

Robert S. von Wolffradt

Robert S. von Wolffradt
Chief Information Officer
State of Iowa

Index: Table of Contents

Background: Introduction

Background:

The recognition that cybersecurity threats can cause catastrophic consequences serves to strengthen the importance of a robust and integrated planning effort for a significant cyber incident. According to a report from the Center for Digital Government "the threats to government entities are so pervasive and sophisticated that anyone can fall victim, particularly as government agencies are strapped for resources. While the above provides information concerning anecdotal examples, statistical data shows an even more startling scenario of the cyber threats with which state and local governments must contend. Consider:

- The total number of records containing sensitive personal information involved in security breaches in the United States was over 608 million records among 3,763 data breaches since January 2005.
- Malicious attacks (defined as a combination of hacking and insider theft) accounted for nearly 47 percent of the recorded breaches in 2012 in the United States. Hacking attacks were responsible for more than one third (33.8 percent) of the data breaches recorded.
- Government agencies have lost more than 94 million records of citizens since 2009.
- The average cost per lost or breached record is $194."[3]

In 2012, former U.S. Secretary of Defense Leon Panetta pointed out our nation's increasing vulnerability to a cyber-attack and the ability that foreign hackers have to disrupt our government, power grid, transportation system and financial networks. He likened the threat to our nation's cyber systems to a "cyber Pearl Harbor."[5]

> ***"The increasing dependency upon information technology systems and networked operations pervades nearly every aspect of our society. While bringing significant benefits, this dependency can also create vulnerabilities to cyber-based threats. Underscoring the importance of safeguarding critical information and information systems and weaknesses in such efforts, federal information security and protecting computerized systems supporting our nation's critical infrastructure are designated a high-risk area."*** [4]

According to a 2013 report from the National Governors Association : "cybersecurity remains one of the most significant challenges facing the nation. Although implementing policies and practices that will make state systems and data more secure will be an iterative and lengthy process, governors can take a number of actions immediately that will help detect and defend against cyber-attacks occurring today and help deter future attacks.

Those actions include:

- Establishing a governance and authority structure for cybersecurity;
- Conducting risk assessments and allocating resources accordingly;
- Implementing continuous vulnerability assessments and threat mitigation practices;
- Ensuring the state complies with current security methodologies and business disciplines in cybersecurity;
- Creating a culture of risk awareness.

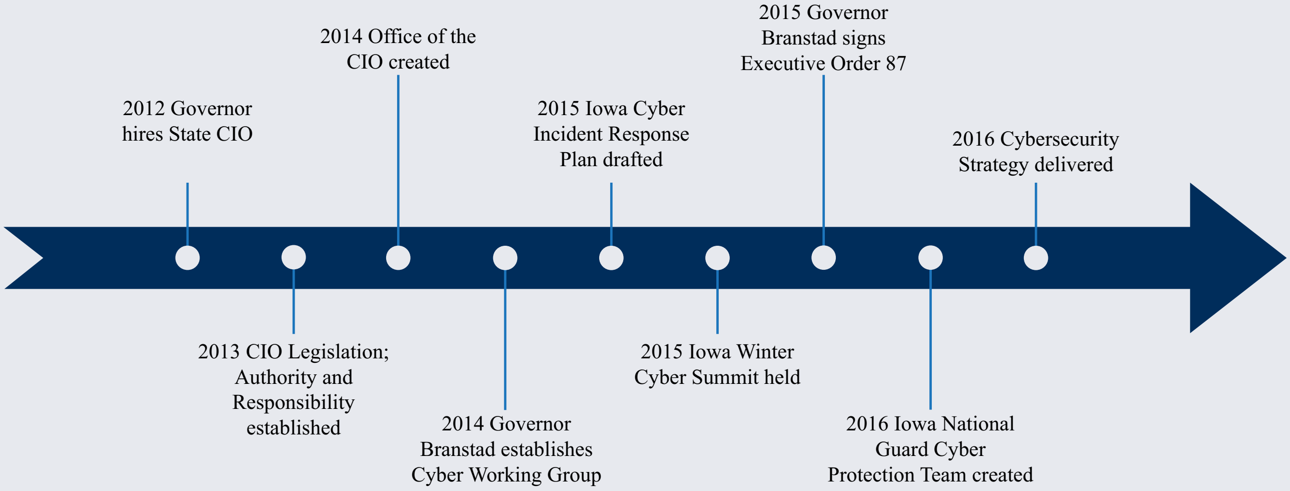
By implementing those recommendations immediately, governors can greatly enhance states' cybersecurity posture."[6]

Current State:

Cybersecurity is a top priority not only in Iowa, but for our nation and throughout the world. It is a threat that affects us all; citizens, governments and businesses. The State of Iowa, like many states and organizations, faces serious challenges in securing our digital infrastructure and information technology systems from cyber-attacks. These attacks not only threaten the critical infrastructure that deliver lifeline services, but can also disrupt the delivery and integrity of government services our citizens are dependent upon.

> ***"Government agencies have lost more than 94 million records of citizens since 2009."***

The State of Iowa is moving in the right direction when it comes to securing our digital infrastructure and information technology systems from cyber-attacks.



2012 Governor hires State CIO
2013 CIO Legislation; Authority and Responsibility established
2014 Office of the CIO created
2014 Governor Branstad establishes Cyber Working Group
2015 Iowa Cyber Incident Response Plan drafted
2015 Iowa Winter Cyber Summit held
2015 Governor Branstad signs Executive Order 87
2016 Iowa National Guard Cyber Protection Team created
2016 Cybersecurity Strategy delivered

The EO87 Leadership Team represents a multi-agency partnership established by the Governor's office because each agency plays a critical role in protecting state government and lifeline critical infrastructures from constant cybersecurity threats. This group will continue to work together to promote and develop solutions to address these cyber-related challenges.

Other partnerships and relationships currently exist today to deal with the persistent threat of cyber-attacks. State agencies work with federal partners, other states, local governments, universities and schools, and the private sector through a variety of venues. Our goal is to enhance, improve, and formalize many of these key existing partnerships as well as identify new avenues for collaboration and partnership to protect Iowans from the persistent threat of cyber-attacks.

EO87 Leadership Team

DPS IAHSEMD ICN ING OCIO

Section 1: Protecting Lifeline Critical Infrastructure

1. Protecting Lifeline Critical Infrastructure:

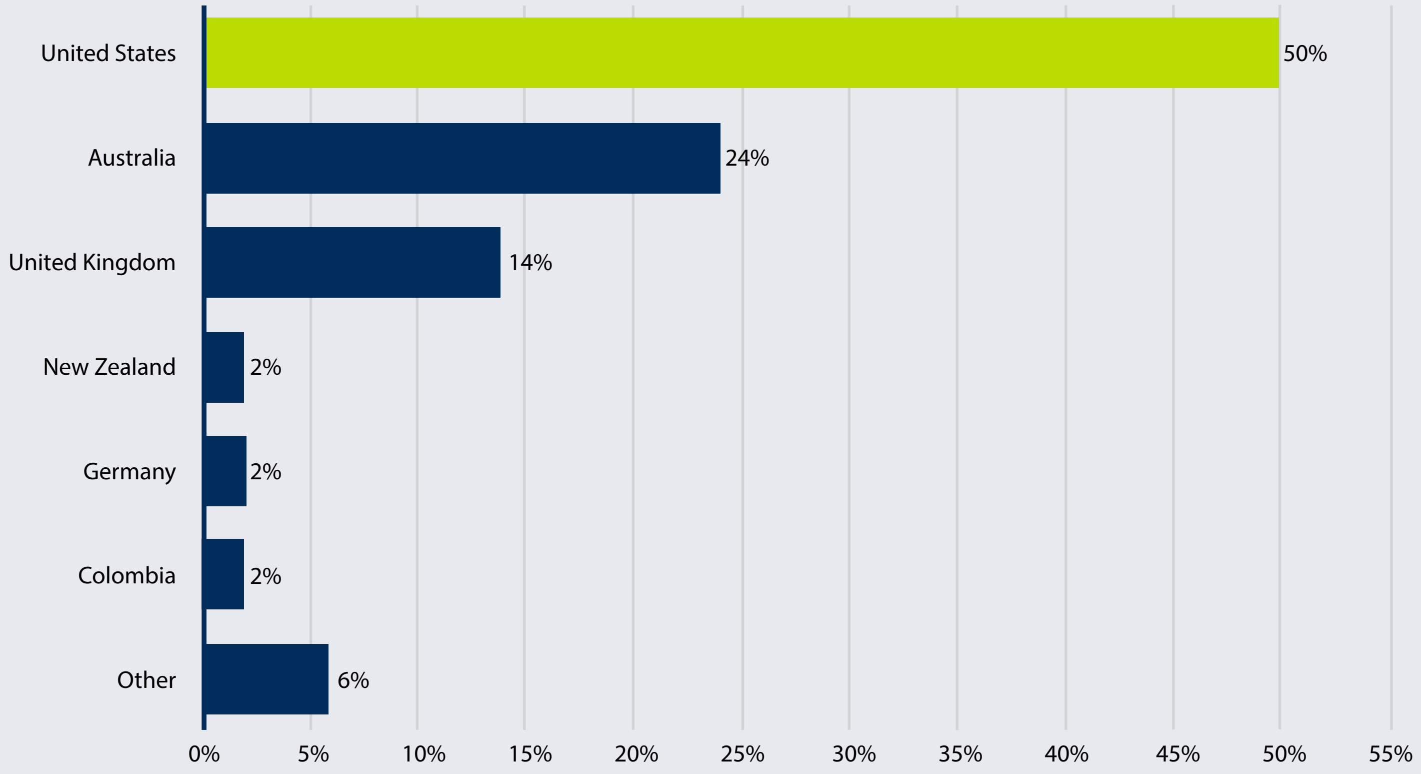
Address high risk cybersecurity areas for the State's critical infrastructure and develop plans to better identify, protect, detect, respond, and recover from significant cyber incidents.

Background:

"The first nation-state warfare took place between soldiers on the ground, and then ships at sea. In the 20th century the battle moved to the skies."[7] The battle is moving to cyberspace. Our national well-being relies upon a secure and resilient infrastructure. Protecting critical infrastructure from cyber-attacks is a global and national need. The chart below shows that 50% of the confirmed cyber-attacks reported in 2014 were targeted against the United States. "Western infrastructure is a target for several kinds of threat actors including, but not limited to, nation-state hackers, cybercriminals, cyber terrorists and hacktivists. A malicious code spread in cyberspace could put the lives of entire populations in danger. The protection of critical infrastructure is a pillar of any government's cyber strategy."[8] National Security Agency Chief Admiral Michael Rogers informed Congress last year that "China and 'probably one or two other' countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber attack..."[9] There is no time to waste when it comes to protecting critical infrastructure.

Share of Cyber-Attacks

(Graph Generated by Statistica - 2016)



Section 1: Protecting Lifeline Critical Infrastructure

A report by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the United States reports that industrial control systems were hit by cyber-attacks at least 245 times over a 12 month period from October 2013 to September 2014. Around 32% of industries were from the energy sector, while critical manufacturing comprised 27%. ICS-CERT further revealed that 55% of investigated incidents showed signs that advanced persistent threats, or targeted attacks, had been used to breach systems.

The State of Iowa is accustomed to responding to natural disasters as they relate to snow storms, floods and tornados. Iowa Homeland Security Emergency Management Department (HSEMD), the Iowa National Guard (ING) and law enforcement respond to these events as part of their ongoing missions in a disaster. These events are sporadic and infrequent when compared to the nature of cyber-attacks. Cyber-attacks are occurring every second of everyday and are capable of disrupting the critical lifeline services we depend on such as the delivery of electricity, water, communications, transportation and fuel distribution.

Lifeline critical infrastructure sectors typically employ production systems called Industrial Control Systems (ICS). ICS are typically used for industrial production purposes in industries such as electric, water and wastewater, oil and natural gas, and the transportation sectors. They typically include electro-mechanical devices that open and close electrical breakers, valves controlling the flow of liquids, or other devices or switches critical to important industrial processes that can be amenable to cyber manipulation.

> ***"There have been, as of this writing, only four secretaries of homeland security. Each of them has conceded the likelihood of a catastrophic cyberattack affecting the power grid; none has developed a plan designed to deal with the aftermath. "*** [10]

Because of the relationship between IT systems and ICS in our state's lifeline critical infrastructure, disruption of any one of the systems during a cyber-attack can create a life-threatening situation to the public. Likewise, because of their interrelated nature, the disruption of any one of the lifeline sectors is likely to have a cascading effect on other critical infrastructure sectors.

Therefore, cyber incidents carry with them the potential for physical consequences such as the actual loss of life or property, civil unrest, or significant impact on the health or economic security of the state. Over 90% of the critical infrastructure is provided by the private sector, and therefore government must play a key role in collaboration, planning and coordinating with these sectors.

In addition to the disruption of lifeline critical infrastructure due to a cyber-attack, a successful cyber-attack against state government can disrupt the delivery of government provided services. This will adversely impact our citizens who depend on these services in their day-to-day lives. Government services which were historically delivered through manual processes have been automated to provide faster and easier access to information and reduce the overall cost of government. Maintaining the confidentiality, integrity and availability of these digital systems is crucial for the State of Iowa.

Current State:

The ability of lifeline critical infrastructure to successfully perform these five functions—to identify, protect, detect, respond, and recover from significant cyber incidents is essential to their ability to manage cybersecurity risk. HSEMD in conjunction with the Department of Public Safety's (DPS) Division of Intelligence and Fusion Center collaborates with the private sector critical infrastructure owners. Iowa Code § 29C.8

(3) (e) requires HSEMD to maintain a list of critical assets including their criticality, vulnerability, and level of threat to the assets. Those critical assets are maintained in conjunction with United States Department of Homeland Security (US-DHS) Office of Infrastructure Protection and the US-DHS Protective Security Advisor and include a cyber vulnerability assessment. HSEMD staff members also meet with lifeline sector partners to discuss the resiliency of their systems and build relationships in advance of a disaster response. Discussions include their area of service, potential impacts, and redundancies in place, and capability or resource gaps that may exist in cases of a cyber-attack or other disaster.

The recently established Iowa Air National Guard Cyber Protection Team (CPT) offers significant potential to assist both the State of Iowa and private sector critical infrastructure in responding to significant cyber events. The CPT has special skills and expertise that can be used to coordinate, train, advise, and assist critical infrastructure partners and state government in developing potential strategies, plans, and solutions for dealing with significant cyber events. Guidelines for utilizing the CPT for cyber preparedness or response are outlined in Appendix E.

The Iowa Utilities Board (IUB) is also actively working with key Iowa utility providers to review cyber capabilities. The IUB is very concerned and engaged in the issue of cybersecurity both with respect to agency operations and the operation of utilities in Iowa. The IUB has previously met with many utilities in Iowa to discuss their efforts in this area and will continue to do so on a regular basis to ensure Iowa utilities are adequately prepared. The IUB participates in agency, state and national efforts in emergency planning and preparedness which includes participation in national discussions on cybersecurity through organizations in which we have members as well as internal and external testing and training exercises. The IUB represents an important conduit of information connecting public utilities with federal, state, local, and industry efforts to share best practices, to respond to threats and to protect our infrastructure.

"A spokesman for the Iowa Utilities Board said the board staff 'has held individual meetings with all utilities and some trade associations in the gas, electric, telecom and water sectors. The participants gave a high level overview of their company cybersecurity efforts and the board staff's understanding is that the utilities have good policies/procedures in place to detect and address the vulnerabilities of the networks to a large extent'."[11]

As part of the State of Iowa's Continuity of Operations and Continuity of Government program (COOP/COG), State of Iowa agencies and offices have identified essential functions they perform and the digital systems used to support those functions. Potential impacts have been determined based upon public health, safety, financial and other key factors. Initiatives are ongoing to ensure the most critical systems are resilient and redundant.

Section 1: Protecting Lifeline Critical Infrastructure

The State of Iowa has forged many key relationships with educational and private sector partners to better identify, protect, detect, respond, and recover from significant cyber incidents affecting high risk critical infrastructure. Safeguard Iowa Partnership and the Iowa InfraGard Chapter serve as conduits for establishing public and private sector partnerships and collaboration. Additionally, the State of Iowa often participates in national and Iowa based cyber exercises such as ISERange, Cyber Prelude, Vigilant Guard and Cyber Storm which may involve both public and private sector organizations.

1. Protecting Lifeline Critical Infrastructure Recommendations:

Recommendation 1.1 – Implement the National Cybersecurity Framework to create a baseline for measuring cybersecurity risk and assessing progress in lifeline critical infrastructure services and state government.

Recommendation 1.2 – Formalize the Iowa Cybersecurity Incident Response Plan and necessary agreements and processes for collaboration between state agencies, and regularly exercise the plan.

Recommendation 1.3 - Continue forging partnerships with lifeline critical infrastructure sectors to ensure the resiliency of digital systems. Promote and facilitate joint training and exercise scenarios.

Recommendation 1.4 – Promote additional public and private assessment processes such as the HSEMD/US-DHS Critical Infrastructure IP Gateway Survey Program and the Iowa Utilities Board cyber reviews.

Recommendation 1.5 – Leverage state resources, such as the Iowa Communications Network pursuant to IAC 8D.9 (3) to test, secure and protect critical communication infrastructure.

Section 2: Risk Assessment

2. Risk Assessment:

Establish a process to regularly assess cybersecurity infrastructure and activities within the State.

Background:

Cybersecurity risk assessments are important because they increase accountability, improve transparency, and educate state government on where to direct limited resources, identify high risk areas, and augment continuity of government initiatives.

According to the U.S. Government Accountability Office (GAO) "… assessing risk is one element of a broader set of risk management activities. Other elements include establishing a central management focal point, implementing appropriate policies and related controls, promoting awareness, and monitoring and evaluating policy and control effectiveness. Although all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected. This continuing cycle of activity, including risk assessment, is illustrated in the following depiction of the risk management cycle."[12]

Current State:

Internal cybersecurity risk assessment processes are not new to the State of Iowa. Within the Office of the Chief Information Officer (OCIO), the Information Security Office (ISO) has conducted cybersecurity risk assessments for the past eight years. The ISO originally utilized the ISO27001 cybersecurity risk assessment framework. It was customized for the state as annual agency compliance status reports were required. In 2014, the Center for Internet Security Critical Security Controls (CIS-CSC) were included in the cybersecurity risk assessment process. In addition to the ISO risk assessments, the Auditor of State utilizes Federal Information Systems Controls Audit Manual (FISCAM) as a framework for auditing state agencies. This is a federal framework from the GAO. A number of state agencies are required to have regular cybersecurity risk assessments as part of their federal compliance responsibilities and also rely on third parties to perform periodic assessments.

In addition to internal cybersecurity risk assessments, the State of Iowa also partners with other government entities and private sector critical infrastructure providers to assist with assessments. The ISO partners with the Iowa County Information Technology (ICIT) Security workgroup to share technology and partner on initiatives and assessments. In conjunction with the United States Department of Homeland Security (US-DHS), Iowa Homeland Security and Emergency Management Department (HSEMD), provides a Critical Infrastructure Protection program that includes a cybersecurity assessment for the private sector partners. Additionally, Safeguard Iowa acts on behalf of HSEMD to create public and private partnerships and facilitate cybersecurity assessments.

These assessments have been used to identify and prioritize several statewide cybersecurity projects and priorities. Based on findings from these assessments, initiatives in the areas of Vulnerability Management, Intrusion Detection, Anti-Malware, and Security Awareness training have been undertaken.

2. Risk Assessment Recommendations:

Recommendation 2.1 – Report annually to the Governor's Office and Iowa Legislature on the current state of cybersecurity risk, COOP/COG, and IT Disaster Recovery readiness for the Executive Branch.

Recommendation 2.2 – Assemble a working group of public and private subject matter experts to evaluate the current risk assessment process and make specific recommendations for improving the overall process.

Recommendation 2.3 – Improve accountability and transparency of state government's cybersecurity posture by creating a cybersecurity risk assessment report card.

Section 3: Best Practices

3. Best Practices:

Provide recommendations related to securing networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destructions of data held by the State of Iowa.

Background:

Iowa's state government is a complex organization with over 35 agencies, elected offices, boards, commissions and two other branches of government. These agencies and entities have a diverse set of missions, priorities, funding streams, and federal obligations. Their digital environment is no less complex or diverse. Many of these systems are intertwined both internally and externally with third party entities such as cities, counties, schools, and the federal government. Additionally, many solutions are provided or supported by third party vendors. What is common among all of these entities is the need for the consistent, accurate and reliable delivery of government services to our citizens and the protection of the data and the digital infrastructure that delivers these services. Initiatives for improving cybersecurity for the State of Iowa and implementing best practices should be viewed as bipartisan in nature and take a risk management approach by prioritizing limited resources to protect the most important digital infrastructure systems first.

Current State:

Implementing cybersecurity best practices has always been a goal of state government. For a number of years, the state has been subject to both internal and external cybersecurity requirements, standards, policies, and audits.

Internally, Executive Branch agencies are subject to periodic audits by the Auditor of State. Findings are published and addressed accordingly. The state's Chief Information Officer (CIO) within the Office of the Chief Information Officer (OCIO) establishes policies and minimum IT standards for state government. Agencies are empowered to implement more stringent security standards to meet additional requirements of their agency. The CIO also prioritizes enterprise security initiatives for state government. A number of key initiatives have been implemented to date. These are selected based upon recommendations from the National Institute of Standards and Technology (NIST) Center for Internet Security – Critical Controls (CIS-CS) findings from annual agency risk assessments.

Many of the state agencies must comply with external cybersecurity requirements as well. Some of these requirements include federal compliance with the Federal Bureau of Investigation Criminal Justice Information Systems (CJIS), the Internal Revenue Service Publication 1075, the Health and Human Services Health Insurance portability and Accountability Act (HIPAA), and the Social Security Administration.

While we strive to meet compliance requirements, we first and foremost focus our efforts on securing the data and applying industry leading best practices. These recommendations are high level and broad in nature. Specific recommendations will be identified in the operational plan to follow.

3. Best Practice Recommendations:

Recommendation 3.1 – Fully implement the CIS-CS Controls for Effective Cyber Defense which offers guidance for securing networks, systems and data with a prioritized risk based approach.

Recommendation 3.2 - Leverage the findings from the 2016 Executive Branch Cybersecurity Survey and create an operational plan, timeline and budget which addresses gaps and prioritizes remediation within the CIS-CS and National Cybersecurity Security Framework.

Recommendation 3.3 – Reduce duplicative security products and initiatives and consolidate resources and solutions under the OCIO.

Section 4: Awareness Training

4. Awareness Training:

Implement cybersecurity awareness training for State government.

Background:

A robust information security awareness training plan is a vital pillar of any information security program. Information security awareness programs address the human element of cybersecurity risks across the multiple roles that interact with digital information.

While it is impossible to prevent every person from falling for a cyber-attack, educating employees has proven to be an effective method of reducing the overall risk. Security technologies exist to reduce and prevent attacks, but are only partial solutions for addressing the overall problem. We must address the human element as well. Requirements for information security awareness training are found in all of the major information security frameworks and federal auditing requirements.

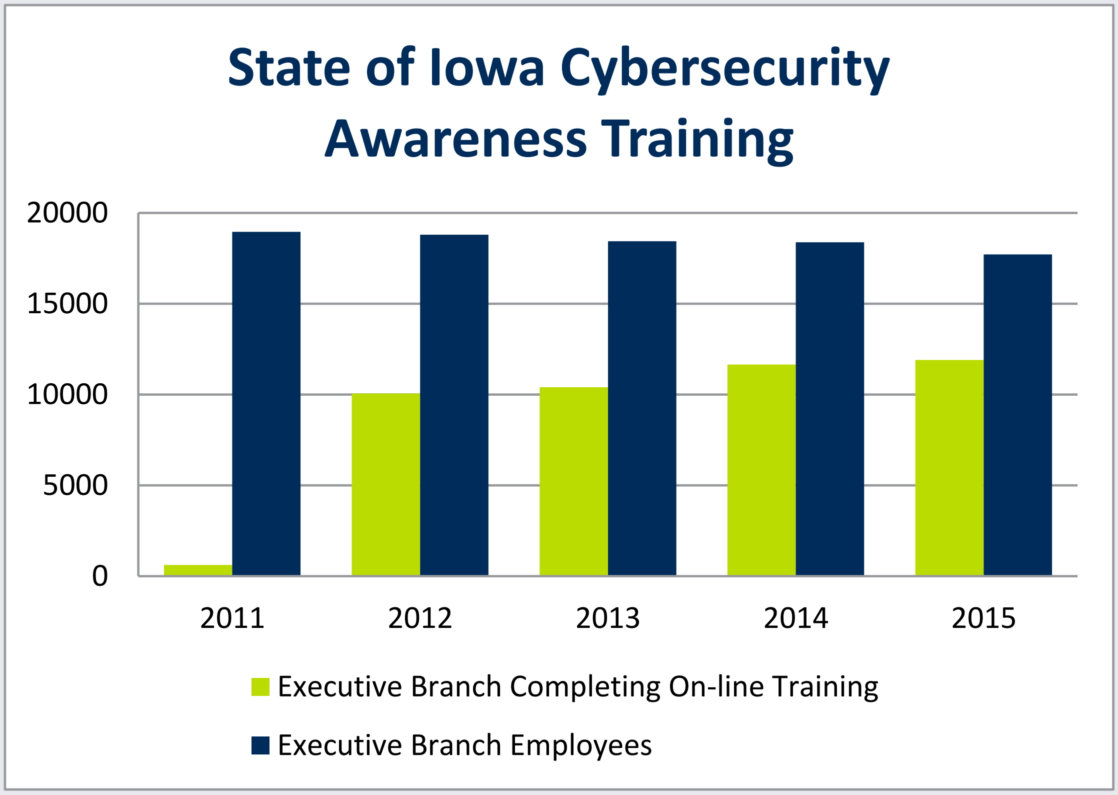
> ***"...the vast majority of hacking attacks are successful because employees click on links in tainted emails, companies fail to apply available patches to known software flaws, or technicians do not configure systems properly."*** [13]

Current State:

Since the inception of the Information Security Office (ISO), cybersecurity awareness training has been and continues to be a key mission of the office. The ISO provides basic information to all state employees as well as customized role-based information to target audiences. The program has evolved over the years and also includes outreach to many local government partners, schools, and non-profits. Many state agencies who are subject to federal audit requirements have built cybersecurity awareness training programs to ensure the proper handling of citizens' private data. Several of these programs predate the Internet.

The ISO serves as the relay point for the distribution of cybersecurity awareness materials distributed by the Multi State Information Sharing and Analysis Center (MS-ISAC), the Federal Trade Commission (FTC), United States Department of Homeland Security (US –DHS), and other organizations. The ISO redistributes materials to targeted audiences, makes training available to all state agencies, cities, and counties, publishes and distributes threat intelligence information, as well as many other activities. The state recently released a Request for Proposal for new cybersecurity awareness training and is identifying new ways to improve the overall cybersecurity literacy of state employees.

As part of the Executive Order 87 initiative, the EO87 Leadership Team surveyed all Executive Branch agencies and invited the elected offices and other branches of government to participate in the process. Based on the survey results and other inquiries in the process, recommendations are as follows.



4. Awareness Training Recommendations:

Recommendation 4.1 – Require general cybersecurity awareness training for all State of Iowa employees and additional specialized cybersecurity awareness training for employees with privileged access. Conduct regular testing to measure the overall effectiveness of the training.

Recommendation 4.2 – Further educate State of Iowa leadership on cybersecurity risk and their roles and responsibilities.

Recommendation 4.3 – Create a cybersecurity training environment to facilitate cross agency training.

Section 5: Public Education and Communication

5. Public Education and Communication:

Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information.

Background:

Cyber criminals, hackers, and malware are thriving in part because too many people are blindly relying on technology as their main line of defense against cyber-attacks. Although necessary, technical security measures like firewalls, patches, and anti-virus software are not completely reliable because cyber criminals have evolved and now focus on human vulnerabilities such as curiosity to accomplish their goals. Simply clicking on an email link, visiting the wrong website, or falling for an email scam can have dire financial consequences and put citizen's privacy at risk. As a result, the decisions that people do and do not make in the course of their daily interactions with information technology often have the greatest effect on the security of their computers and the confidentiality of their personal information. The State of Iowa is in a position to play a leadership role in developing and disseminating materials to every citizen on how to take an active role in their own cyber defense.

"When asked why they don't always do all the things they can or should do to stay safer online, Americans said they simply lacked the information or knowledge (28 percent) - a surprising finding that surpassed other hurdles often cited by the media. Only 12 percent said online safety was too expensive, while just 5 percent said they were too busy to take the extra step.

Concern about identity theft rates slightly higher than fears of job and healthcare loss. 54 percent of Americans are extremely concerned about loss of personal or financial information. To place this is in context, 53 percent are concerned about losing their jobs, while 51 percent feared not being able to provide healthcare for their family.

Nearly two-thirds of the American public have heard, read or seen something about online safety and security issues recently. However, most of what the news they remember is negative: identity theft, privacy loss, and increased frequency of attacks."[14]

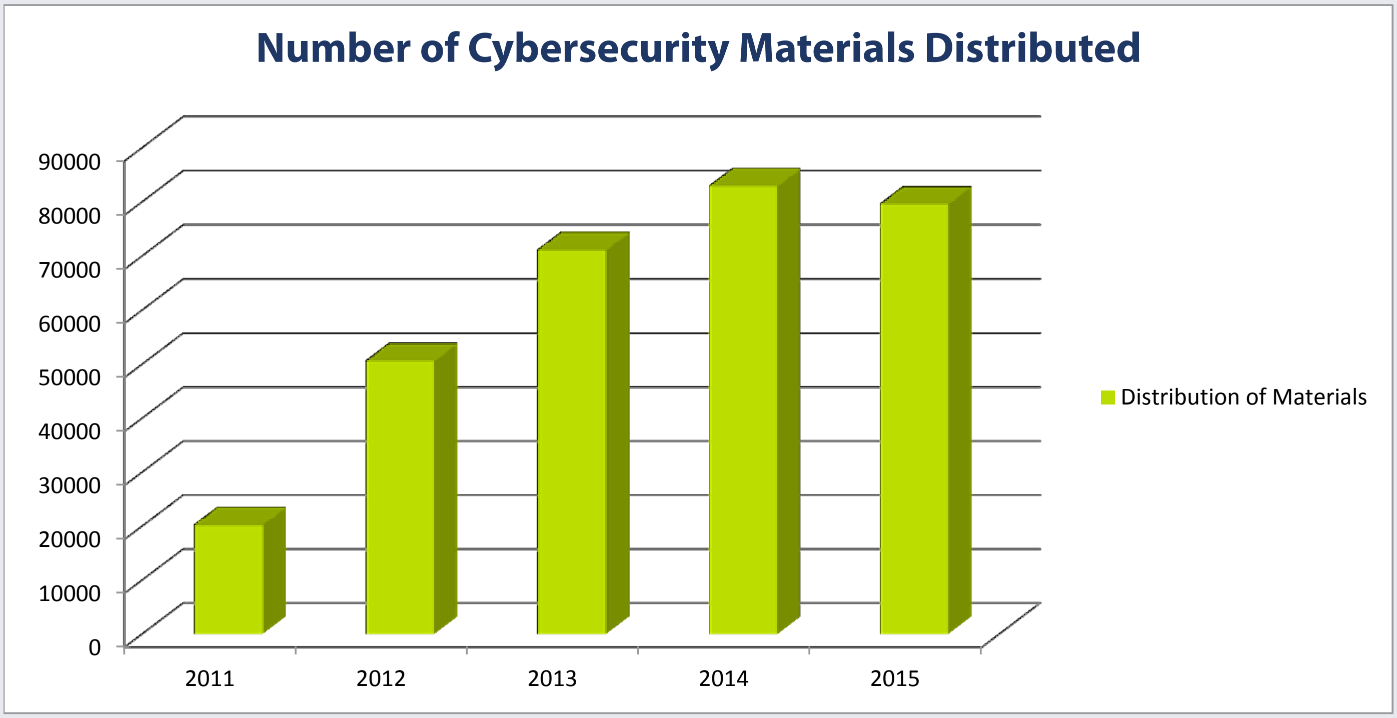
Current State:

Both the Iowa State Patrol and the Division of Criminal Investigation's Internet Crimes Against Children (ICAC) Task Force provide educational presentations on Internet safety. Approximately 1,700 presentations are conducted annually reaching over 44,000 Iowans.

The State of Iowa Information Security Office (ISO) educates individuals in state and local government, K-12 schools, the business community and the public about cybersecurity best practices and cyber-threats.

The ISO distributes Security News about emerging cyber-threats and security best practices to 1500+ individuals annually in the public and private sectors and hosts in-person cybersecurity training sessions for state and local government and educators. Online security awareness training was made available to K-12 educators and public librarians to help raise awareness about the importance of good cybersecurity practices. The ISO also provides speakers on a regular basis for information security conferences and events.

Security best practice guides and awareness handouts are distributed to state agencies, public universities, counties, cities, K-12 school districts, Area Education Agencies, community colleges, municipal utilities, and public libraries during cybersecurity awareness month in October and throughout the year.



5. Public Education & Communication Recommendations:

Recommendation 5.1 – Institute a public cybersecurity awareness and literacy campaign to improve the cybersecurity awareness of Iowans and promote good cyber hygiene.

Recommendation 5.2 – Facilitate and sponsor an annual public and private cybersecurity conference.

Recommendation 5.3 - Provide cybersecurity awareness and literacy curricula and support materials for K-12 and college students.

Section 6: Collaboration

6. Collaboration:

Collaborate with the private sector and educational institutions to implement cybersecurity best practices.

Background:

Collaboration is a key element to any cybersecurity strategy. By working with government, and education and industry partners, the group can enhance the overall security of the state. Information sharing is critical to address the advanced cyber- threats facing the state. Such collaboration can include:

- Sharing threat intelligence
- Preparedness training and exercises
- Best of breed solutions

"Everyone has a collective responsibility for the security of the Internet: multistakeholder cross-border collaboration is an essential component. Commercial competition, politics and personal motivation play a role in how well collaboration happens. But, as collaborative efforts have demonstrated, differences can be overcome to cooperate against a threat. Such voluntary as-needed 'working for the benefit of everyone' collaboration is remarkable for its scalability and its ability to adapt to changing conditions and evolving threats, yielding unprecedented efficacy."[15]

Current State:

The State of Iowa Information Security Office (ISO) collaborates with federal, state and local government entities on numerous cybersecurity efforts. These include participation in national workgroups, specific cybersecurity projects, information sharing, and multi-agency exercises to name a few. Some of the groups the ISO collaborates with include: Safeguard Iowa, InfraGard, Technology Association of Iowa, Multi-State Information Sharing & Analysis Center (MS-ISAC), Iowa County Information Technology (ICIT), Board of Regents Information Security (BORIS), and Iowa State University Cybersecurity Advisory Council. The ISO supports MS-ISAC efforts to reach out to local government and the public and has worked with universities to train state and local government IT staff in network protection, cyberterrorism defense and incident response.

6. Collaboration Recommendations:

Recommendation 6.1 – Improve and enhance current partnerships with educational institutions to identify cybersecurity best practices through internships and faculty expertise.

Recommendation 6.2 – Conduct cybersecurity training exercises across Executive Branch agencies and lifeline critical infrastructure sector partners.

Recommendation 6.3 – Identify, create, review and update legal agreements between collaborative partners to improve information sharing, preparedness and incident response.

Recommendation 6.4 - Expand private sector partnership programs to promote the sharing of criminal and cyber-threat information affecting the private sector in Iowa.

7. STEM:

Recommend Science, Technology, Engineering, and Math (STEM) educational and training programs for K-12 and higher educational programs in order to foster an improved cybersecurity workforce pipeline.

Background:

"In the government and government-related job sector, certain STEM disciplines have a shortage of positions at the Ph.D. level (e.g., materials science engineering, nuclear engineering) and in general (e.g., systems engineers, cybersecurity, and intelligence professionals) due to the U.S. citizenship requirement."[16]

"Under any strategy, a state will need a cyber workforce with a wide array of skills, from proficiency in higher order information science to risk assessment to behavioral sciences and a variety of less demanding skills, such as those necessary to reinforce the practice of cyber hygiene day in and day out. The state will have to compete with other governmental employers and private-sector employers in the market for cybersecurity workers. That market is diffuse and complex and best thought of as an amalgamation of many smaller labor markets for skilled workers. In each of those markets, the willingness of public and private sector employers to pay, and of workers to respond to such inducement, will be among the key determinants of the level of cybersecurity afforded to a state or a business."[17]

HYPERSTREAM
THE TECH HUB FOR IOWA STUDENTS

Information regarding STEM can be found at Iowastem.gov. The need for additional STEM workers along with the need for a cybersecurity workforce is well documented. In order to increase the number of workers there needs to be an increase in the number of students focused on cybersecurity.

ISEAGE
Internet-Scale Event and Attack Generation Environment

"Of the 30 fastest-growing occupations projected through 2016, the U.S. Bureau of Labor Statistics' Occupational Outlook Handbook concludes that 16 require substantial mathematics or science preparation. Despite the numbers of graduates coming out of universities in the state, more must be done to encourage students to consider cybersecurity careers and prepare for work in the field. There are two issues: universities need to attract American-born students into IT programs, and students must be aware obtaining a security clearance requires smart and safe lifestyle decisions. "[18]

What is at stake is far greater than the privacy of an individual, but instead the protection of our critical infrastructure systems, intellectual property, strength of our economy and national security.

IT-ADVENTURES
MAKING IT FUN

Current State:

Iowa State University (ISU) is recognized by the National Security Agency as one of the first seven Centers for Excellence.

Section 7: STEM

ISU participates in the National Science Foundation Scholarships for Service (SFS) program to support students working in Information Assurance. Program participants will take courses in information assurance as part of their regular degree requirements. In addition, all scholarship recipients will become part of an SFS cohort group and participate in academic and social activities throughout the year. The scholarship also requires a service commitment consisting of a paid summer internship and two years of paid employment with a state or federal agency. The fellowship includes all tuition, room, board, books and fees, as well as an annual stipend for 2 years of an MS degree or 3 three years of a Ph.D. degree. ISU received its initial funding for the SFS program in 2001 and has received three renewals (total funding for the program to date is over $8,000,000). The SFS (Cyber Corps) Fellowship program at ISU has supported over 75 students studying Information Assurance.

Hyperstream and the IT-Olympics is a partnership between ISU and the Technology Association of Iowa created in 2008. The program is designed to allow Iowa high school clubs to explore and draw awareness of IT among high school students using inquiry-based learning which allows students to explore IT in a nonthreatening, experimental environment. The program has developed four content areas that the clubs have the opportunity to explore: cyber defense, robotics, application development, and multimedia. This is accomplished through a large group of IT professionals and school instructors dedicated to be the mentors for clubs during the year. To celebrate at the end of the school year, the clubs are invited to ISU for a two day event to participate in the four areas in fun. This program has held statewide cyber defense competitions for over 10 years with the goal of increasing the number of students entering the computer security field. The Hyperstream and IT-Olympics program is currently in over 200 schools across the state of Iowa. ISU has developed a cybersecurity curriculum for high schools that is based off of our cybersecurity playground called ISERink. This playground and corresponding curriculum enable high school students to explore cybersecurity.

ISU along with Des Moines Area Community College have been working on developing pathways for students interested in cybersecurity from high schools to enter either a community college for 2 year education or on to a 4 year school. These pathways will be a model for cooperation between high schools, community colleges and ISU with the goal of increasing the number of students graduating with a degree in cybersecurity.

7. STEM Recommendations:

Recommendation 7.1 – Incentivize Iowa students to pursue careers in cybersecurity through the creation of scholarship programs modeled after programs such as the Federal Cyber Corps; Scholarship for Service program, the AmeriCorps Model, the Military GI Bill, and others.

Recommendation 7.2 – Provide and encourage pathways to cybersecurity careers from K-12 through higher education.

Recommendation 7.3 – Conduct a review of the cybersecurity workforce requirements for the Executive Branch and recommend necessary adjustments.

8. Data Breach:

Establish data breach reporting and notification requirements.

Background:

"Forty-seven states and the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information."[19] This includes Iowa.

These laws were designed to protect citizens of each state by notifying them if their Personally Identifiable Information (PII) had been stolen. PII often includes financial information, social security numbers, driver's license numbers, credit card and medical information. Studies have shown that every industry sector is subject to a data breach and depending on the type of data breach, the reporting and notifications can vary. It is critical to reduce the time between a breach being discovered to the time of reporting and notification to the impacted public. This reduces the potential damage which can occur to a citizen's private information and allows the public to take steps to protect themselves from further harm. In order to reduce the impact of a privacy breach, plans and appropriate laws must be in place before a data breach occurs. Data breach reporting also allows the security industry and government to measure the overall scope of the problem in order to allocate the necessary resources.

Although a national data breach law and database have been discussed, there are currently no standard requirements. Each state maintains their own notification requirements.

Current State:

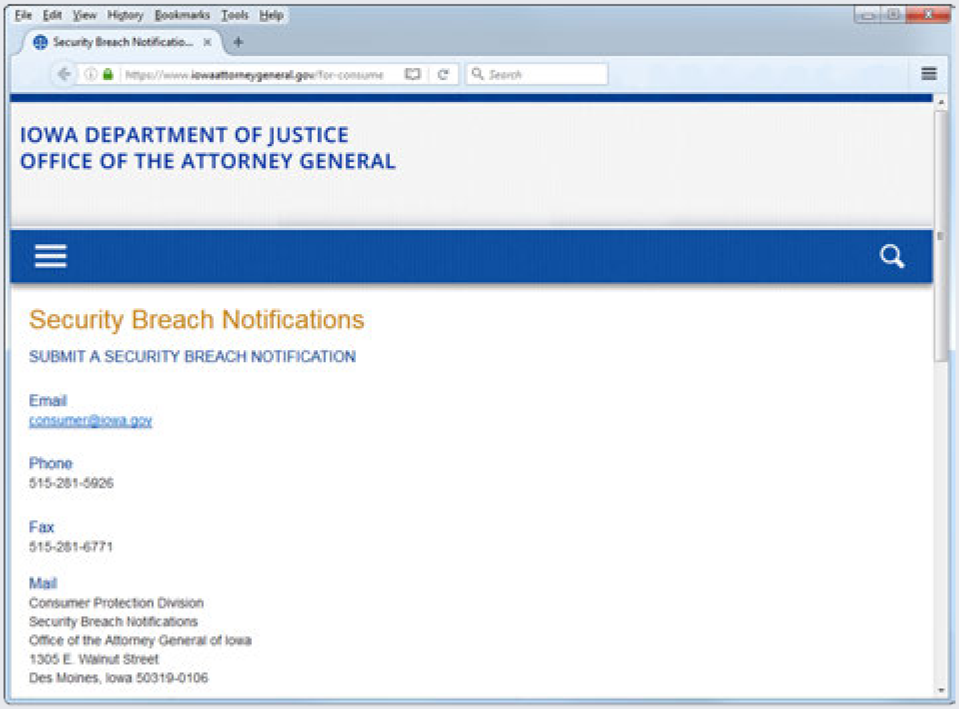
Iowa's Security Breach Notification Law enacted in 2008 and codified at Iowa Code Chapter 715C imposes, among other things, an obligation on persons who own or license computerized data containing Iowa residents' "personal information," as defined by the statute, and which is the subject of a security breach, to notify the affected residents of, among other things, the fact of and circumstances related to the security breach. The law was subsequently amended in 2014 to:

1. Expand the definition of "Breach of security" to include certain paper breaches;
2. Narrow the encryption safe harbor to be unavailable when encryption keys related to the improperly acquired information were also obtained through the security breach;
3. Require the owner or licensor of the adversely affected data to notify the consumer protection division of the attorney general's office of significant security breaches (defined as security breaches affecting five hundred or more Iowa residents).

Reporting a Data Breach - The Attorney General's Website:

https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/

Section 8: Data Breach


File Edit View History Bookmarks Tools Help
Security Breach Notificatio...
https://www.iowaattorneygeneral.gov/for-consume
Search

IOWA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

Security Breach Notifications

SUBMIT A SECURITY BREACH NOTIFICATION

Email
consumer@iowa.gov

Phone
515-281-5926

Fax
515-281-6771

Mail
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Email:
consumer@iowa.gov

Phone:
515-281-5926

Fax:
515-281-6771

Mail:
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General
of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Notwithstanding the legislative changes in 2014, recent increases in the occurrence of significant security breaches nationwide and observed legislative trends in other states to improve the force and efficacy of comparable security breach notification laws suggest that additional changes to Iowa's Security Breach Notification Law are needed. See Appendix B for additional details.

8. Data Breach Recommendations:

Recommendation 8.1 – Work with the Iowa Attorney General to introduce changes to Iowa's Code Chapter 715C which would facilitate greater insight into the security breaches occurring in the state and better protect the personal information of the citizens of Iowa.

Recommendation 8.2 – Participate in initiatives designed to standardize data breach notification requirements at a national level to aid in the protection of citizen privacy and establish consolidated standards and reporting.

Recommendation 8.3 – Track and report the data breach impact to citizens of Iowa and Iowa businesses.

Iowa Emergency Response Plan – Cyber Annex:

The Iowa Homeland Security and Emergency Management Department shall update the State's Emergency Response Plan to deal with the physical consequences of a significant cyberattack against the State's critical infrastructure.

"Having an incident response team can reduce the cost of a data breach by nearly $400,000 on average, the study's authors said. Moreover, speed makes a difference. The study found that the average time to identify a breach was 201 days; the average time to contain it was 70 days.

In general, breaches that were identified in fewer than 100 days cost companies an average of $3.23 million, whereas those found after the 100-day mark cost $4.38 million.

Companies with business continuity management (BCM) processes in place were ahead there, discovering breaches 52 days earlier and containing them 36 days faster than companies without, according to the study's authors."[20]

"Having an incident response team can reduce the cost of a data breach by nearly $400,000 ..."

Typically, the emergency response to natural disasters starts at the local level and additional resources are added by higher levels of government as the need arises. The mantra that all disasters are local is particularly true for natural disasters in the sense that the disaster response begins and ends at the local level and that the cause of the disaster is a localized weather phenomenon or other local event. In the case of a typical natural disaster, there may be small need for information sharing with the federal government.

A significant cyber incident caused by a nation-state or other foreign actor will be different. The consequences will be felt locally—albeit on a widespread basis in the case of an attack against the electrical grid—but the cause of the attack may originate far from the point of impact or damage. Sharing information about the nature of the cyber-attack, its scope, and remediation techniques will be critically important.

In order to recover from the incident or remediate the effects of the attack on a local system, information about the nature of the attack and additional attacks, and the experience of those also affected by the attack will be important. That type of intelligence information may well rest with federal authorities and their willingness to share that information may dictate how quickly local systems recover DPS Intelligence and Fusion Center will disseminate threat and mitigation information to private sector partners.

The Iowa Emergency Response Plan includes instructions, policies, and explanatory information related to many or all of the entities involved in emergency or disaster response, as well as information about the legal and administrative foundations for state emergency response, plan activation requirements, and the structure of the response organization.

Iowa Homeland Security and Emergency Management Department (HSEMD) maintains and updates the

Iowa Emergency Response Plan. The plan detailing the state's response to a significant cyber-attack against the state's lifeline critical infrastructure should be set out in a Cyber Annex to the Iowa Emergency Response Plan. The Cyber Annex will follow the Iowa Cyber Incident Response Plan (ICIRP) drafted by the Cyber Working Group formed by Governor Branstad in December 2014.

Iowa Cyber Incident Response Plan:

The ICIRP should set out the overall plan the State of Iowa will follow to coordinate an incident response to a significant cyber incident or attack against the State of Iowa's information technology systems and services or the systems or services belonging to the state's broader lifeline critical infrastructures.

These significant cyber incidents by definition carry with them the potential for physical consequences such as the actual loss of life or property, civil unrest, or significant impact on the health or economic security of the state.

General roles and responsibilities included in the plan:

- Office of the Chief Information Officer (OCIO) should lead state government in protecting information technology resources by identifying, protecting, detecting, responding and recovering from cybersecurity events and incidents through its Cybersecurity Incident Response Plan.

- HSEMD should serve as the state's lead in responding to the physical consequences of any significant cyber event under the state's Emergency Response Plan.

- Department of Public Safety (DPS) through its Intelligence Fusion Center and Cyber Crime Unit should provide threat and mitigation assistance to the private sector as well as acting to investigate, attribute, and prosecute cybercrimes.

- Iowa Communication Network (ICN), as the State of Iowa's primary broadband carrier, provides and manages Internet, network infrastructure and transport services. At the direction of the OCIO, the ICN will take actions to isolate the state's IT systems from cyber-attacks pursuant to its Network Security Incident Response Plan.

- Iowa National Guard through its Air Guard Computer Protection Team (CPT) will support the State of Iowa in responding to a significant cyber incident.

Overall Incident Command:

The overall coordination of the cyber aspects of a significant cyber incident should vest in the coordinating entity that would deal with cyber recovery and remediation matter. The response to the physical consequences of a significant cyber event would be coordinated by HSEMD pursuant to its emergency response plan.

In addition to relevant State of Iowa agencies, the entity should include representatives from the Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), US Computer Emergency Readiness Team (US-CERT), and representatives from the affected critical infrastructure.

Federal partners that should be made part of any cyber response plan:

- The U.S. Department of Homeland Security (US-DHS) through its Office of Cybersecurity and Communications coordinates the national effort for the protection, prevention, mitigation of, and recovery from cyber incidents. US-DHS also disseminates domestic cyber threat and vulnerability analysis involving critical infrastructure through the National Cybersecurity and Communications Integration Center (NCCIC) and staffs the U.S. Computer Emergency Readiness Team (US-CERT). US-DHS's Industrial Control System Cyber Emergency Response Team (ICS-CERT) has special expertise with cyber-attacks involving industrial control systems.

- Department of Justice Federal Bureau of Investigation (FBI) leads domestic national security operations in respect to cyber incidents. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat intelligence and mitigation methods and investigates, attributes, and prosecutes cybercrimes.

- The Department of Defense (DoD) supports the national protection, prevention, mitigation of, and recovery from cyber incidents. In addition to protecting national security and military systems, the DoD, acting through the U.S. Cyber Command defends the nation from cyber-attacks. One of the goals of the Iowa Air National Guard Cyber Protection Team is to support U.S. Cyber Command in its mission.

- Multi-State Information Sharing and Analysis Center (MS-ISAC) in Albany, New York, works with the US-DHS NCCIC to provide cyber threat prevention, protection, response and recovery for the State of Iowa and local governments.

- US-DHS Office of Infrastructure Protection working with HSEMD and the DPS Intelligence Fusion Center and utilizing the IP Gateway system can share critical infrastructure-related cyber information through the Protected Critical Infrastructure Information system in a way that protects that information from disclosure to those that would seek to misuse that information.

Cyber Annex Recommendations:

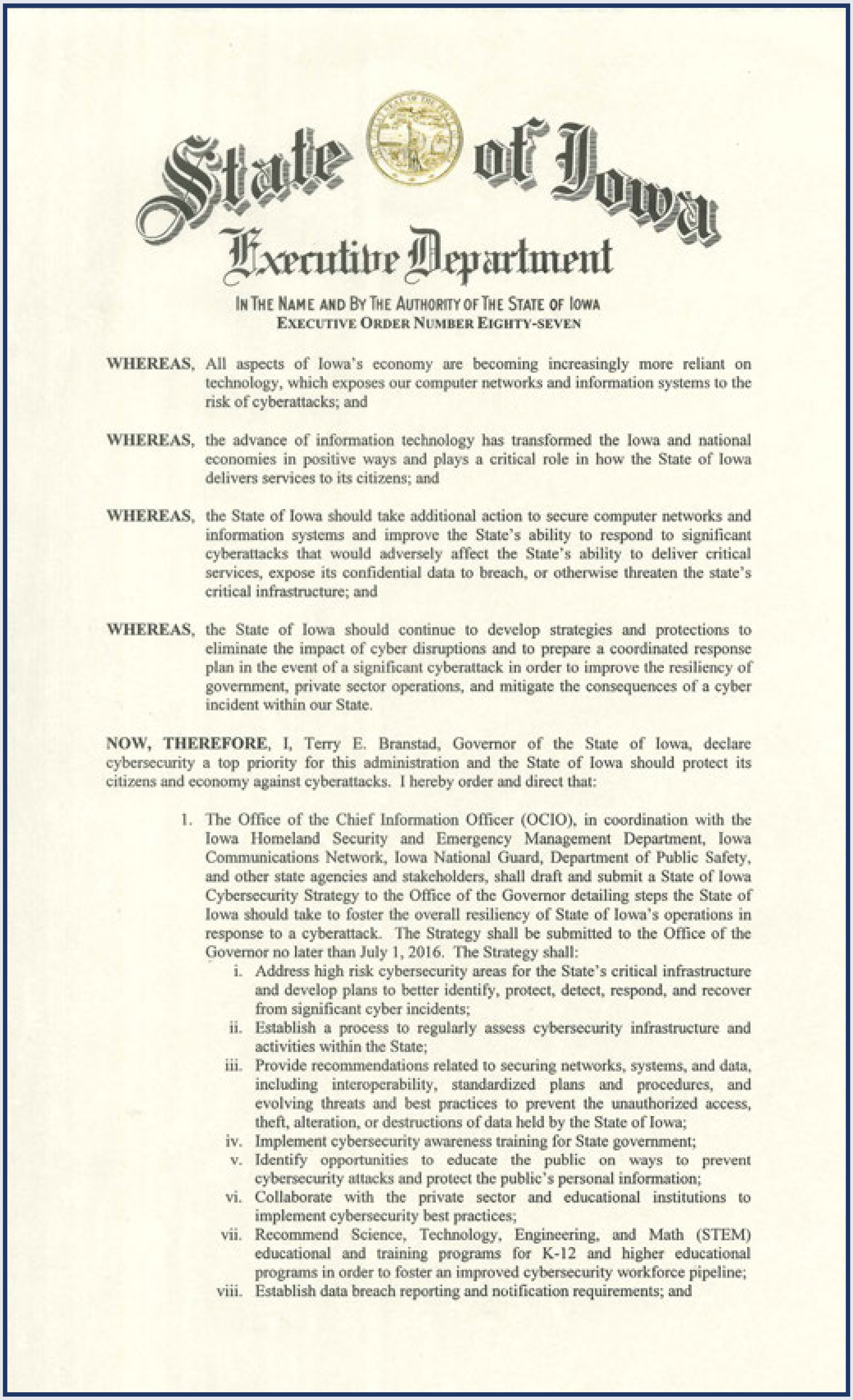
Recommendation CA 1 - Develop a strategic direction on how the state prepares and responds when cyber-incidents involving lifeline critical infrastructure or state government escalate to a level of significance requiring a coordinated response from a State of Iowa and/or HSEMD perspective.

Recommendation CA 2 - Define a process to manage significant cyber incidents and provide a basis for continuing refinement of our processes and policies that address the path from steady-state to incident response.

Recommendation CA 3 - Formalize the Cyber Annex of the State of Iowa Emergency Response Plan and the Iowa Cyber Incident Response Plan with required reviews and updates every two years.

Recommendation CA 4 - Exercise the Cyber Annex as part of the State of Iowa Emergency Response Plan and the Iowa Cyber Incident Response Plan.

Appendix A : Executive Order 87



State of Iowa

Executive Department

IN THE NAME AND BY THE AUTHORITY OF THE STATE OF IOWA
EXECUTIVE ORDER NUMBER EIGHTY-SEVEN

WHEREAS, All aspects of Iowa's economy are becoming increasingly more reliant on technology, which exposes our computer networks and information systems to the risk of cyberattacks; and

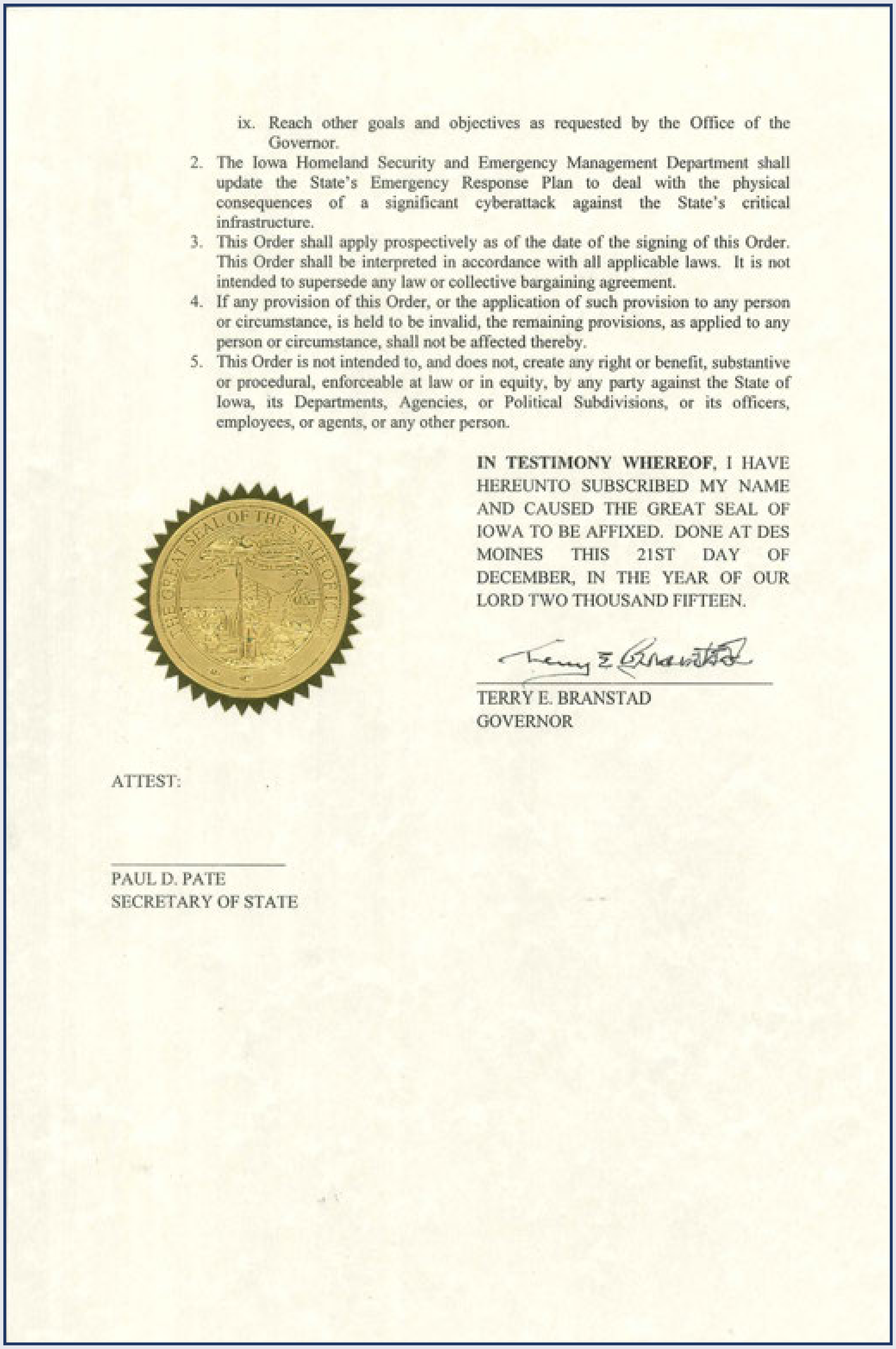
WHEREAS, the advance of information technology has transformed the Iowa and national economies in positive ways and plays a critical role in how the State of Iowa delivers services to its citizens; and

WHEREAS, the State of Iowa should take additional action to secure computer networks and information systems and improve the State's ability to respond to significant cyberattacks that would adversely affect the State's ability to deliver critical services, expose its confidential data to breach, or otherwise threaten the state's critical infrastructure; and

WHEREAS, the State of Iowa should continue to develop strategies and protections to eliminate the impact of cyber disruptions and to prepare a coordinated response plan in the event of a significant cyberattack in order to improve the resiliency of government, private sector operations, and mitigate the consequences of a cyber incident within our State.

NOW, THEREFORE, I, Terry E. Branstad, Governor of the State of Iowa, declare cybersecurity a top priority for this administration and the State of Iowa should protect its citizens and economy against cyberattacks. I hereby order and direct that:

1. The Office of the Chief Information Officer (OCIO), in coordination with the Iowa Homeland Security and Emergency Management Department, Iowa Communications Network, Iowa National Guard, Department of Public Safety, and other state agencies and stakeholders, shall draft and submit a State of Iowa Cybersecurity Strategy to the Office of the Governor detailing steps the State of Iowa should take to foster the overall resiliency of State of Iowa's operations in response to a cyberattack. The Strategy shall be submitted to the Office of the Governor no later than July 1, 2016. The Strategy shall:
   - i. Address high risk cybersecurity areas for the State's critical infrastructure and develop plans to better identify, protect, detect, respond, and recover from significant cyber incidents;
   - ii. Establish a process to regularly assess cybersecurity infrastructure and activities within the State;
   - iii. Provide recommendations related to securing networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, or destructions of data held by the State of Iowa;
   - iv. Implement cybersecurity awareness training for State government;
   - v. Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information;
   - vi. Collaborate with the private sector and educational institutions to implement cybersecurity best practices;
   - vii. Recommend Science, Technology, Engineering, and Math (STEM) educational and training programs for K-12 and higher educational programs in order to foster an improved cybersecurity workforce pipeline;
   - viii. Establish data breach reporting and notification requirements; and



ix. Reach other goals and objectives as requested by the Office of the Governor.

2. The Iowa Homeland Security and Emergency Management Department shall update the State's Emergency Response Plan to deal with the physical consequences of a significant cyberattack against the State's critical infrastructure.
3. This Order shall apply prospectively as of the date of the signing of this Order. This Order shall be interpreted in accordance with all applicable laws. It is not intended to supersede any law or collective bargaining agreement.
4. If any provision of this Order, or the application of such provision to any person or circumstance, is held to be invalid, the remaining provisions, as applied to any person or circumstance, shall not be affected thereby.
5. This Order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the State of Iowa, its Departments, Agencies, or Political Subdivisions, or its officers, employees, or agents, or any other person.

IN TESTIMONY WHEREOF, I HAVE HEREUNTO SUBSCRIBED MY NAME AND CAUSED THE GREAT SEAL OF IOWA TO BE AFFIXED. DONE AT DES MOINES THIS 21ST DAY OF DECEMBER, IN THE YEAR OF OUR LORD TWO THOUSAND FIFTEEN.

Terry E. Branstad

TERRY E. BRANSTAD
GOVERNOR

ATTEST:

PAUL D. PATE
SECRETARY OF STATE

Download Executive Order 87:
https://governor.iowa.gov/sites/default/files/documents/Executive%20Order%20No.%2087.pdf

Appendix B : Breach Legislation

A High Level Overview of the Legislative Changes to Iowa Code Chapter 715C Proposed in This Document.

Notwithstanding the legislative changes in 2014, recent increases in the occurrence of significant security breaches nationwide and observed legislative trends in other states to improve the force and efficacy of comparable security breach notification laws suggest that additional changes to Iowa's Security Breach Notification Law would facilitate greater insight into the security breaches occurring in the state and better protect the personal information of the citizens of Iowa.

Consistent with these objectives and the legislative changes observed in other states, the attached proposed legislative changes would, among other things:

1. Expand the definition of "Breach of security" to include not only cases where the owner or licensor of personal information has actual knowledge that personal information has been acquired by an unauthorized person, but also cases where the owner or licensor possesses a reasonable belief that personal information has been acquired by an unauthorized person;

2. Expand the definition of "Breach of security" and related provisions to apply to all paper breaches;

3. Establish a minimum encryption threshold, 128 bit or higher, in order to qualify for the encryption safe harbor;

4. Expand the definition of personal information to include:

   a. Financial account number, credit card number, or debit card numbers acquired alone, as opposed to in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account as currently required;

   b. Credit card numbers obtained alone, as opposed to in combination with an individual's first name or first initial and last name;

   c. Medical information;

   d. Health insurance information;

   e. Tax identification numbers;

   f. Individuals' username or email addresses, in combination with a password or security question and answer that would permit access to an online account.

5. Impose a 45-day deadline on the consumer notification requirements following a data breach;

6. Narrow the "no reasonable likelihood of financial harm" exception to require a showing of "no reasonable likelihood of harm," as opposed to "financial harm," in order to qualify for the exception;

7. Clarify that notification to the consumer protection division of the attorney general's office is required in

cases involving significant security breaches, regardless of whether consumer notification is required by Iowa Code Chapter 715C itself or other bodies of law that may otherwise exempt the owner or licensor of personal information from compliance with select provisions of Iowa Code Chapter 715C;

8. Require that already required documented findings that a security breach is not reasonably likely to cause harm to consumers be provided to the consumer protection division of the Attorney General's office;

9. This change specifies what must be included in the notice sent to the Attorney General;

10. Require those who own, license, maintain, or possess Iowa resident's personal information to implement reasonable security measures to safeguard such information;

11. This change authorizes a private right of action for this Chapter, in line with what is normally available to consumers in the circumstance of a Consumer Fraud Act violation;

12. Include the Office of the Chief Information Officer in any data breach notifications made to the consumer protection division of the Attorney General.

Appendix C: General Financial Considerations

The EO87 Leadership Team identified numerous recommendations to improve the cybersecurity posture of the state and protect the private data of the citizens of Iowa. Presenting a strategy without acknowledging the potential need for funding would be incomplete. Figure 1 identifies the EO87 elements where cybersecurity investments may be needed in support, tools and staffing. We intend to provide specific details during the normal budgeting cycle.

While funding and staffing needs to be addressed, we also believe savings can be achieved by eliminating duplication in both tools and staffing effort. Financial recommendations will be based upon risk and the criticality of the infrastructure and government systems. Understanding that protecting everything equally is not fiscally feasible or reasonable; any requests will be measured and specific. Specific spending on cybersecurity is not tracked and will require additional data gathering from individual agencies.

Figure 1:

EO87 References	Investments needed?	Cyber Defense Tools needed?	Cyber Defense Staffing & Partners needed?
1. Protecting Lifeline Critical Infrastructure	Yes	Yes	Yes
2. Risk Assessment	Yes	Yes	Yes
3. Best Practices	Yes	Yes	Yes
4. Awareness Training	No	No	Yes
5. Public Education & Communication	Yes	No	Yes
6. Collaboration	Yes	No	Yes
7. STEM	Yes	No	Yes
8. Data Breach	No	No	No
Iowa Emergency Response Plan - Cyber Annex	No	No	No

Appendix D: General Legislative Considerations

During the development of the cybersecurity strategy, the need for updates to the Iowa Code was identified. While specific language will need to be drafted, the following are areas which may need legislative changes to provide and assist in the protection of State of Iowa's digital infrastructure.

Figure 2:

EO87 Element	Updates	State of Iowa Code
1. Protecting Lifeline Critical Infrastructure	Yes	29C
2. Risk Assessment	Yes	2.x, 8B
3. Best Practices	Yes	8B
4. Awareness Training	No	
5. Public Education & Communication	Yes	8B
6. Collaboration	No	
7. STEM	May	
8. Data Breach	Yes	88.x
Cybersecurity and open records considerations	Yes	22

Appendix E: Iowa National Guard

The world of cyber has been, is and will continue to change and develop rapidly. How, when, where and the extent of incident responders' involvement in responding to a cyber incident is difficult to predict. With that in mind, below is some general guidance and analytical tools to consider when employing Iowa National Guard (ING) personnel in response to a cyber incident.

The primary mission of the Iowa Air National Guard Cyber Protection Team (CPT): Coordinate, Train, Advise and Assist (CTAA) support and services must be military training with incidental benefit to mission partners. Coordination with mission partners to protect DoD Information Network, enhance awareness, provide mission assurance and provide unity of effort is appropriate. The ability and extent to which CPT CTAA support and services is available is dependent upon the nature of the mission partner (non-governmental v. governmental). DoD guidance with respect to all requests for assistance must be strictly adhered to. Prior to providing CPT CTAA support and assistance to mission partners, a memorandum of agreement (MOA) between the Iowa Air National Guard (IANG) and mission partner will be required. Further, the IANG is not a replacement for mission partner's responsibilities to maintain and employ its own IT subject matter experts, and to ensure security measures to protect the integrity of their computer networks. MOA must generally contain provisions including but not limited disclaimers of liability, non-disclosure agreements, reimbursement provisions (as applicable), scope and terms of services, third-party permissions, Proprietary Intellectual Property Methods and Protocols, contract termination terms, cost reimbursement (if applicable), modification terms and duration of the MOA.

Support provided by the ING while in state active duty (SAD) to state/local civil authorities for emergencies/operations is state funded under the provisions of state law. States are free to employ their National Guard (NG) forces under state control for state purposes and at state expense as provided in the state's constitution and statutes. As such, service is performed in accordance with state law, ING members performing this type of duty are said to be in SAD status. National Guard Soldiers and Airmen serving in a SAD status are under the command and control of the Governor and the state or territorial government.

Support provided by the ING under the command of the Governor, funded by DoD (Title 32). T32 Funding for Other Duty. Section 502(f) of T32 has been used to allow members of the NG to be ordered to full-time National Guard duty to perform training or operational activities. This section provides that "a member of the ING may ... without his consent, but with the pay and allowances provided by law ... be ordered to perform training or other duty" in addition to those they are already prescribed to perform. This is the provision of law which was used to provide federal pay and benefits to National Guard personnel who provided security at many of the nation's airports after September 11, 2001, and who participated in Hurricanes Katrina and Rita-related disaster relief operations. In accordance with 32 USC 502(f) (2), the President or Secretary of Defense may request operations or missions to be performed under the authority of Section 502(f).

State governments bear all of the associated costs of NG members performing duties in a state active duty status per NG Regulation 500-5/ Air National Guard Instruction 10-208, Chapter 10, 10-2. Governors can directly access and utilize the NG's federally assigned aircraft, vehicles, and other equipment (subject to some restrictions based on federal law and regulation) so long as the federal government is reimbursed for the use of the equipment and supplies. There are specific reporting and reimbursement procedures and requirements to the federal government for the use of federal equipment or expenditure of federal supplies. NG forces are unique in their ability to operate under a spectrum of federal and state statutes and authorities including Titles 10, 18, 32 and 50; U.S.C. Based on the breadth of authorities and their community-based presence across the nation, the NG provides significant capability to facilitate work across federal, state, and private sector boundaries. In addition, NG uniqueness is also reflected in their routine interactions with both the private and public sectors. NG members typically have strong and enduring linkage at local, city, county, and state levels, based not only on their private sector positions and experience, but also on their state and local role as responders and incident managers during state and local emergencies under their Governor's authorities. SAD is governed by Iowa law, particularly Article VI of the Iowa Constitution and Iowa Code sections 29A.7 and 29A.8.

DoDD 3025.10 provides that "the authority of state officials is recognized to direct a state immediate response using NG personnel under State command and control (including personnel in a T32, U.S.C. status) in accordance with State law…."[21] As the principle authority during state emergencies, governors may direct an immediate response using NG personnel under state command and control (including personnel in a T32 status); however, NG personnel will not be placed in or extended in T32 status to conduct State immediate response activities. Additionally, state leadership must coordinate with the Chief of the National Guard Bureau to approve the continued use of personnel in a T32 status responding in accordance with immediate response authority in excess of seventy-two hours. Before deploying any forces in support on civilian authorities a Commander in consultation with their JAG must consider the following criteria set out in DoDD 3025.18.

These criteria are known as the "CARRLL" factors:

- **Cost –** Who pays and the impact on DoD budget.
- **Appropriateness –** Whether it is in the interest of DoD to provide the requested support.
- **Readiness –** Impact on DoD's ability to perform its primary mission.
- **Risk –** Safety of DoD forces.
- **Legality –** Compliance with the law.
- **Lethality –** Potential use of lethal force by or against DoD forces.

Appendix F: Glossary of Acronyms

- **BORIS –** Board of Regents Information Security
- **CARRLL –** Cost, Appropriateness, Readiness, Risk, Legality, Lethality
- **CIO –** Chief Information Officer
- **CIS –** Critical Information Security
- **CIS-CSC –** Center for Internet Security – Critical Security Controls
- **CJIS -** Criminal Justice Information Systems
- **COOP/COG –** Continuity of Operations/Continuity of Government
- **CPT -** Cyber Protection Team
- **CTAA -** Coordinate, Train, Advise and Assist
- **US-DHS –** United States -Department of Homeland Security
- **DoD –** Department of Defense
- **DPS –** Department of Public Safety
- **EO –** Executive Order
- **FBI –** Federal Bureau of Investigation
- **FTC –** Federal Trade Commission
- **FISCAM -** Federal Information Systems Controls Audit Manual
- **GAO –** Government Accountability Office
- **HSEMD –** Homeland Security Emergency Management Department
- **HIPAA –**Health Insurance Portability and Accountability Act
- **IANG –** Iowa Air National Guard
- **ICAC –** Internet Crimes Against Children
- **ICIRP –** Iowa Cyber Incident Response Plan
- **ICIT –** Iowa County Information Technology
- **ICN –** Iowa Communications Network
- **ICS –** Industrial Control System
- **ICS-CERT –** Industrial Control Systems– Cyber Emergency Response Team
- **ING –** Iowa National Guard
- **ISEAGE –** Internet Scale Event & Attack Generation Environment
- **ISO –** Information Security Office
- **ISU –** Iowa State University
- **IT –** Information Technology
- **IUB –** Iowa Utilities Board
- **MOA –** Memorandum of Agreement
- **MS-ISAC –** Multi-State Information Sharing and Analysis Center
- **NCCIC -** National Cybersecurity and Communications Integration Center
- **NG –** National Guard
- **NIST –** National Institute of Standards & Technology
- **OCIO –** Office of the Chief Information Officer
- **PII –** Personally Identifiable Information
- **SAD –** State Active Duty
- **SFS –** Scholarship for Service
- **STEM –** Science, Technology, Engineering and Math
- **US-CERT –** U.S. Computer Emergency Readiness Team

Appendix G: References

1. http://publications.iowa.gov/21403/1/Executive%20Order%20No%2087.pdf

2. http://www.computerworld.com/article/3083916/security/cost-of-a-data-breach-4m-benefits-of-responding-quickly-priceless.html

3. Data Breaches in the Government Sector, Rapid7, 2012: http://www.nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20Local%20Government.pdf

4. http://www.gao.gov/key_issues/cybersecurity/issue_summary

5. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0

6. http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf

7. Time Magazine. *March 24, 2016.*

8. http://www.foxnews.com/tech/2016/02/15/why-protecting-critical-infrastructure-from-cyberattacks-is-global-emergency.html

9. http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/

10. Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath by Ted Koppel: https://www.goodreads.com/work/quotes/44848451-lights-out-a-cyberattack-a-nation-unprepared-surviv-ing-the-aftermath

11. http://www.eenews.net/stories/1059999027

12. http://www.gao.gov/special.pubs/ai00033.pdf

13. http://www.reuters.com/article/usa-cybersecurity-idUSL2N0XB01K20150414

14. https://www.stopthinkconnect.org/research-surveys/research-findings

15. http://www.internetsociety.org/collaborativesecurity

16. http://www.bls.gov/opub/mlr/2015/article/stem-crisis-or-stem-surplus-yes-and-yes.htm

17. http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1410TheCybersecurityWorkforce.pdf

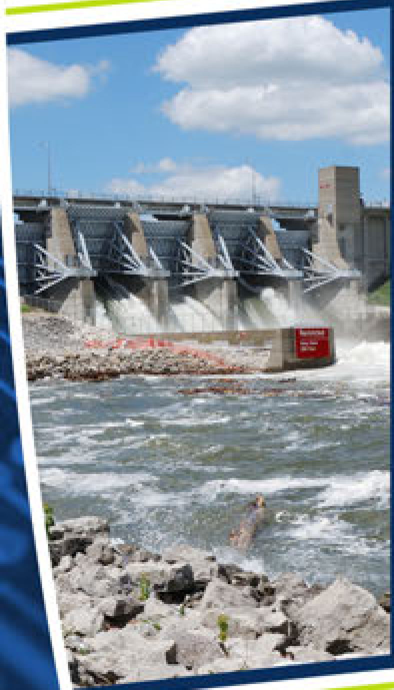
18. http://commerce.maryland.gov/Documents/ResearchDocument/CybermarylandReport.pdf

19. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notifi-cation-laws.aspx

20. http://www.computerworld.com/article/3083916/security/cost-of-a-data-breach-4m-benefits-of-responding-quickly-priceless.html

21. http://www.dtic.mil/whs/directives/corres/pdf/302518p.pdf

Notes



Revised 8/5/2016