THIRD WAY

Cyber Enforcement in Four Key States

by Brandon Gaskew

In the range of national security challenges facing US presidential administrations, only a few involve a foreign adversary causing harm to an American without ever leaving their country—it's cyber. According to a Pew Survey on global threats, Americans rank foreign cyberattacks as their top threat, ahead of even terrorism.[1] And it's no wonder. America is facing a cybercrime wave and it is getting bigger every year–undermining America's national security and affecting every sector of the economy. In the aggregate, cybercrime costs the US economy up to $109 billion and trillions globally. [2] From cyber vulnerabilities of America's military weapons, to the theft of America's intellectual property, to election interference, to the ransomware used to cripple US cities, to the financial crimes and identity thefts that affect average Americans, the range of cybercrime and cybercriminals is vast.[3]

The 2020 presidential election offers an opportunity for Americans to raise concerns about cybercrime and draw attention to cybersecurity at a state and local level. To help inform these discussions, Third Way has prepared this memo to educate candidates about the growing national security threat of cybercrime, and the resources that have been created in four key states to tackle the threat: Iowa, New Hampshire, Nevada, and South Carolina. 2020 presidential candidates should use the information in this memo to elevate the conversation on cybercrime and develop a national cyber strategy to protect the American people.

This memo contains two components:

- First, it provides a brief overview of the cybercrime threat to the United States and what law enforcement can do to combat it. According to US government data, the most vulnerable victim population is those over age 60.[4] While the states with the largest victim populations are California, Florida, and Texas, there is no state or jurisdiction, without a victim of a cybercrime.[5] Sadly, the vast majority of cybercrimes go unprosecuted. According to Third Way's assessment of the US federal government's own data, only 3 in 1,000 cybercrimes ever see an arrest.[6] Worse, only 1 in 6 cybercrimes are reported, meaning that the chances that a cybercriminal gets caught are miniscule.[7] America can and should do better.
- Second, it showcases how cybercrime has impacted victims in four key states—Iowa, New Hampshire, Nevada, and South Carolina—and the resources those states have established to reduce cybercrime and boost cybersecurity. We analyze who the victims are and what institutions in those states are fighting this growing cybercrime wave to guide the cyber discussion as attention draws to those states.

Third Way's broader report "To Catch a Hacker" [8] contains further recommendations for policy areas that current and future US presidents must focus on to making progress in reducing cybercrime.[9]

Cybercrime in the United States

The United States is facing a cybercrime wave that continues to cause increasing costs to America's national and economic security.

In 2017, over 300,000 cybercrime incidents were reported to the Federal Bureau of Investigation (FBI) — which is likely a vast undercount since many victims do not report their victimization.[10] The ubiquity of technology means every critical infrastructure sector in the United States—from nuclear power plants to water facilities— utilizes some form of computer-enabled system for their operations that, if attacked successfully, could have devastating impacts on Americans. That is why the US Department of Treasury has designated cyber incidents as one of the biggest threats to the stability of the entire US financial system.[11]

Despite the scope and size of the cybercrime threat, Third Way uncovered a stunning cyber enforcement gap, allowing cybercriminals to operate with near impunity. Only 3 out of 1,000 malicious cyber incidents in the United States annually see an arrest, which is an enforcement rate of less than 1%.[12] By comparison, the clearance rate for property crime was approximately 18% and for violent crimes 46%, according to the FBI's Uniform Crime Report for 2016.[13]

Government is the only institution with the authority to pursue human cybercriminals and bring them to justice. However, in the United States, a heavy focus of cyber policy discussions has been building better cyber defenses against intrusion. There is no discussion as to how the government can also impose consequences on cybercriminals that continue to attack Americans and our institutions in every state. **To close the cyber enforcement gap, the United States needs a comprehensive strategy for strengthening the US government's abilities to identify, stop, and punish cybercriminals and other malicious cyber actors, which the country does not currently have.**

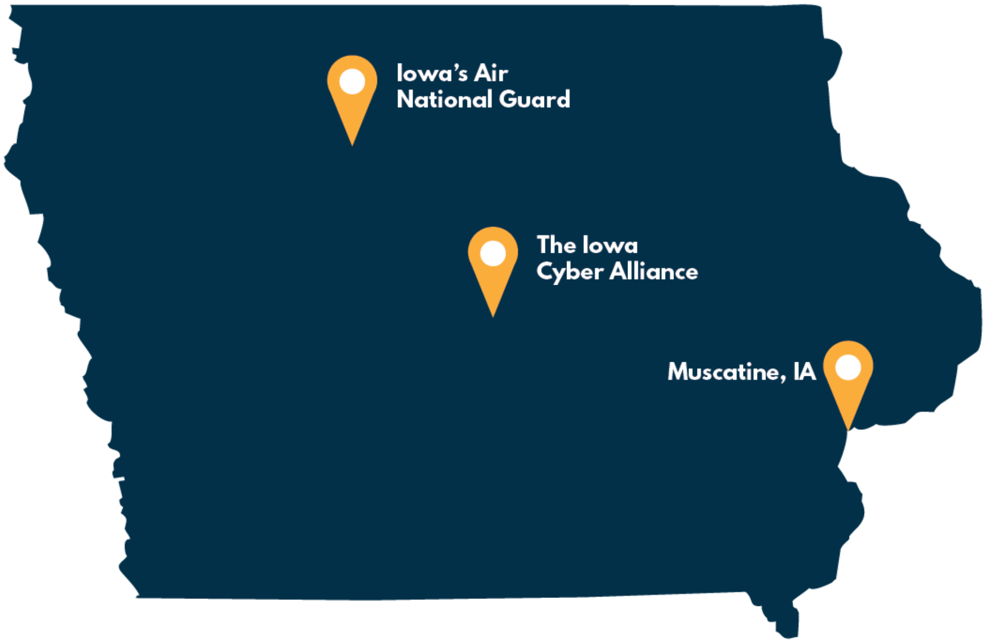
The 2020 US presidential election offers an opportunity for Americans to raise concerns about cybercrime and hear from candidates on all sides about their views. Fortunately, states across the country are directing cyber resources to protect their residents, local businesses, government institutions, organizations, and critical infrastructure from cybercrime and help to support investigations. State and local law enforcement agencies are creating specialized cybercrime units, cyber fusion centers are being setup to share cyber threat intelligence, and public-private partnerships are creating cyber incident response plans.

As attention draws to Iowa, New Hampshire, Nevada, and South Carolina, this is an opportunity to showcase how cybercrime has impacted residents in those states and the work that is happening to protect against and combat the threat at a state and local level. In order to take decisive action to address the national and economic security impacts of malicious cyber activity on Americans, it helps to look through a state and local lens.

Cyber Resources: Iowa

THIRD WAY

Recommended Cyber Resources to Visit in Iowa



Overview of Iowa's Cyber Response

In 2016[14] and 2017,[15] over 1,500 Iowans reported internet crime complaints to the FBI. In 2017, Iowans reported a financial loss of over $4 million[16] to cybercrime.[17]

Iowa began to fortify its cyber resources starting in 2012. Then, former Governor Terry Branstad hired Iowa's first Chief Information Officer (CIO) to manage and coordinate the cyber resources of the state government.[18] In 2015, former Governor Branstad directed the CIO to partner with the Iowa National Guard, Iowa Homeland Security and Emergency Management Department, Iowa Communications Network, the Department of Public Safety, and other key partners to respond to cyber incidents in the state.[19]

As many states mobilize their cyber resources, here are three unique measures Iowa developed to improve its response to cyberattacks:

- **Created cyber education programs:** Iowa State University in partnership with the Iowa National Guard and the state's Office of the Chief Information Officer established the Iowa Cyber Alliance, the nation's first cybersecurity program dedicated to education, outreach, and training of government agencies, businesses, and all its citizens on cyber threats protection.[20]
- **Instituted public-private cyber partnerships:** Organizations like the Safeguard Iowa Partnership, a coalition of business and government leaders, work to facilitate assessments

that have been used to identify and prioritize statewide cybersecurity projects[21] and provide extensive cybersecurity awareness resources to the public.[22]

- **Established a cyber-quarterback to coordinate and manage resources:** Iowa created an Office of the Chief Information Officer as an independent agency to lead and coordinate Iowa's cyber resources, giving it authority to establish information technology (IT) standards used by state agencies, direct agency IT staff, and recommend approval of IT employment decisions with the Iowa Department of Management.[23]

Recent Iowa Cyberattacks

The Office of the Iowa Attorney General maintains an online database[24] of company data breaches from 2011 onwards.[25] Here are recent examples of the impact cyberattacks can have on local municipalities and businesses:

Local Government

- On October 22, 2018, Muscatine County computer networks were hit by the same ransomware that hit the city of Muscatine a few days prior. It prevented police officers from accessing their mobile computers in their squad cars, and the county jail lost access to files linking the National Crime Information Center database.[26]
- On October 18, 2018, the city of Muscatine was hit by a cyberattack.[27] Muscatine government servers were hit with ransomware[28] that paralyzed city services. Tasks as simple as paying for parking tickets or checking books out of the public library were unavailable.[29]

Medical

- In August 2018, Iowa-based Jones Eye Clinic was hit by a ransomware attack that compromised as many as 40,000 patients' information.[30] Information as sensitive as patients' medical record numbers, addresses, and general description of clinic visits was potentially stolen.
- On July 30, 2018, UnityPoint, one of Iowa's main hospitals was hit by a cyberattack that impacted nearly 1.4 million patients.[31] The hackers used a phishing email to access UnityPoint's network, potentially giving the hackers access to patients' medical information.

Education

- In October 2017, the Johnston school district was targeted by a hacker group, resulting in student names, addresses, and telephone numbers being posted online.[32]

Recommended Cyber Resources to Visit

Third Way has identified three vital stops in Iowa that showcase how malicious cyber activity has impacted Iowa and two measures Iowa is taking to protect residents and critical infrastructure from the cyber threat:

- **The Iowa Cyber Alliance** is an organization led by Iowa State University and housed in its Information Assurance Center. It is the nation's first program dedicated to providing cybersecurity education, outreach, and training to government agencies, businesses, and all Iowans.[33]

- **Iowa's Air National Guard** has been mobilized as an important state cyber resource through the Iowa Air National Guard Cyber Protection Team (CPT) to assist the government of Iowa and private sector critical infrastructure in responding to cyber incidents.[34] The CPT is officially the 168th Cyberspace Operations Squadron within the 132nd Wing.[35]
- **Muscatine, IA**, with a population of roughly 24,000, was the target of a cyberattack in October 2018. City servers were infected with ransomware, grinding city services to a halt. Tasks as simple as paying for parking tickets or checking books out of the public library were unavailable to residents.[36]

Key Iowa State and Federal Government Cyber Entities

Local, state, and federal government agencies have a vital role in protecting residents from cyberattack and bringing cybercriminals that attack Americans to justice. Third Way has compiled a list of these entities:

State Cyber Entities

- **Office of the Chief Information Officer (CIO):** The CIO has centralized authority over Iowa state agencies' information technology (IT). It approves IT standards for state agencies and can recommend and review approval of IT professionals at those state agencies.[37]
- **Iowa Information Security Division (ISD):** ISD is led by the Iowa CIO and has responsibility to respond to major cyberattacks and partners with federal, state, and non-profit cybersecurity organizations, including the US Department of Homeland Security and Iowa Homeland Security and Emergency Management.[38]
- **Iowa Department of Public Safety (DPS):** DPS serves as Iowa's state law enforcement agency. The Division of Criminal Investigation houses the Cybercrime Unit, which is responsible for conducting cybercrime investigations. [39]
- **Iowa Communications Network (ICN):** ICN is an independent state agency that administers Iowa's statewide fiber optic telecommunications network. ICN provides firewall service to protect against unauthorized network access, incident response, network security testing, and protection against cyberattacks.[40]
- **Iowa Homeland Security and Emergency Management Department (HSEMD):** HSEMD's mission is to lead and coordinate Iowa's response to homeland security and emergency incidents.[41]
- **Iowa Attorney General (AG):** The Iowa AG is the chief legal officer of the state. Under Iowa law, any security breach that affects at least 500 Iowa residents' companies must provide written notice to the AG's Consumer Protection Division Director within five business days. The AG also maintains a database online of security breaches from 2011 onwards.[42]
- **Iowa National Guard:** The Iowa Air National Guard Cyber Protection Team assists the government of Iowa and private sector critical infrastructure in responding to cyber incidents.[43]

Federal Entities

There are not many federal law enforcement agencies with field offices in Iowa. The only notable entities are a Secret Service field Office located in Des Moines, IA and two US Attorney's Offices:

- **US Attorney's Office for the Southern District of Iowa:** The US Attorney's Office is headquartered in Des Moines, Iowa's largest city. The Office has a Criminal Division responsible for prosecuting any cybercrimes that occur within the district. [44]
- **US Attorney's Office for the Northern District of Iowa:** The US Attorney's Office is headquartered in Cedar Rapids, Iowa's second largest city. The Office has a Criminal Division responsible for prosecuting any cybercrimes that occur within the district.[45]

University Cyber Centers

To effectively address cyberattacks, local, state, and federal entities need trained cyber professionals. There are 299,000 unfilled cybersecurity positions in the United States and the gap is expected to reach 1.8 million by 2022, according to a 2018 report authored jointly by the Department of Commerce and DHS. [46] The gap in unfilled cybersecurity positions covers both the private and public sectors and vacancies range from IT specialists to law enforcement cyber investigators. The large vacancy in positions affects the government and companies' ability to improve their cybersecurity and law enforcement's ability to go after cybercriminals.[47] Universities are taking a lead in addressing this cyber workforce shortage and are creating cyber centers to provide education and training resources for the next generation of cyber professionals.

Here is a list of Iowa universities that have created cyber centers:

- **Eastern Iowa Community College (EICC) Cyber Center:** EICC established their Cyber Center to meet regional demands for cybersecurity education and training.[48]
- **Iowa Cyber Hub:** Iowa State University and Des Moines Area Community College (DMACC) formed the Iowa Cyber Hub in partnership. It is designed to be the focal point for cybersecurity education, outreach, training, and to foster additional interaction between companies and partner schools through internships, training opportunities, and focused projects.[49]
- **Iowa State University Information Assurance Center (IAC):** The IAC is a multidisciplinary center with a mission to conduct comprehensive cybersecurity research, training and education, cybersecurity employment pathways, security literacy and outreach for all Iowans, and partnerships with government and industry.[50]

Military Installations in Iowa

States are using their National Guard units to combat the growing national security threat of cyberattacks. National Guard units are being organized into cyber mission teams. Some are tasked with protecting state-level interests, and others are under the direction of US Cyber Command and are charged with protecting Department of Defense networks and national critical infrastructure.[51] There are currently 3,880 National Guardsmen assigned to cyber service, spread across 59 cyber units in 38 states.[52]

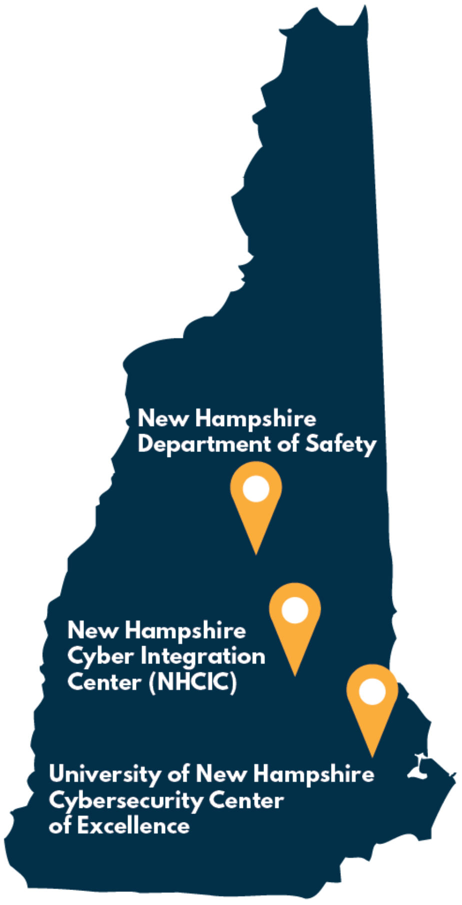
Here are all the major military installations in Iowa:

- Camp Dodge, Johnston, IA (Headquarters of the Iowa National Guard)
- Fort Des Moines, Des Moines, IA
- Iowa Army Plant, Des Moines County, IA

Cyber Resources: New Hampshire

THIRD WAY

Recommended Cyber Resources to Visit in New Hampshire


New Hampshire Department of Safety
New Hampshire Cyber Integration Center (NHCIC)
University of New Hampshire Cybersecurity Center of Excellence

Overview of New Hampshire's Cyber Response

In 2016 and 2017, over 1,100 New Hampshirites reported internet crime complaints to the FBI.[53] The financial impact of cyberattacks on New Hampshire is increasing every year. In 2016, New Hampshirites reported to the FBI a financial loss of $3.1 million,[54] and in 2017 over $3.7 million[55] due to cybercrime.[56]

In 2016 New Hampshire created the New Hampshire Cyber Integration Center (NHCIC) to serve as the statewide focal point for cybersecurity monitoring, information sharing, and threat analysis.[57]

As many states mobilize their cyber resources, here are two unique measures New Hampshire developed to improve its ability to respond to cyberattacks:

- **Created a cybersecurity alert system:** The State of New Hampshire operates a cybersecurity alert level on their website that is updated daily with threat information from the New Hampshire Information and Analysis Center.[58] This is invaluable information that citizens, businesses, and local governments can use to assess the cyber threat level daily.

- **Established a state cyber department to coordinate and manage resources:** New Hampshire has unified all its cyber resources into one organization. The Department of Information Technology is led by a Commissioner and has legal authority to manage and coordinate all technology resources for the state government.[59]

Examples of Recent New Hampshire Cyberattacks

Cyberattacks have hit every sector of the US economy. Here are recent examples of the impact cyberattacks have had on local municipalities and businesses in New Hampshire:

Government

- In April 2018, an energy utility company that supplies power to Massachusetts, Connecticut, and New Hampshire was hit by a cyberattack. It fortunately did not compromise any customers data or disrupt service; however, it did affect the energy company's ability to process some transactions.[60] The damage in this cyberattack was minimal, but if an attack disrupted power across New England, the consequences would be grave for those residents.
- In March 2018, Portsmouth, New Hampshire's city computer system was infected with malware. The cyberattack caused emails to be sent purporting to be city officials, asking recipients to pay a city invoice and instructing them to open a link for further details.[61]

Business

- In 2016, Dyn, based in Manchester, New Hampshire, which provides services to websites like Twitter, Netflix, and Visa, was hit by a cyberattack disrupting internet service across the East Coast.[62]

Education

- In April 2015, the Concord School District was hit by a cyberattack, compromising the W-2 forms of everyone who received payment from the school in 2015. Some of the stolen information was used to file fraudulent tax returns.[63]

Recommended Cyber Resources to Visit

Third Way has identified three vital stops in New Hampshire. One stop was the victim of a cyberattack and showcases how malicious cyber activity has impacted New Hampshire. The other two stops are measures New Hampshire is taking is taking to protect residents and critical infrastructure from the cyber threat:

- **New Hampshire Cyber Integration Center (NHCIC):** The NHCIC serves as New Hampshire's focal point for coordinating cybersecurity monitoring, information sharing, and threat analysis.[64]
- **New Hampshire Department of Safety:** The Major Crimes Unit within the Investigative Services Bureau has computer crime investigators that handle many of the New Hampshire's cybercrime investigations.[65]

- **University of New Hampshire Cybersecurity Center of Excellence:** The Cyber Center partners with academia, industry, and government. Its mission is to educate cybersecurity professionals on technical and societal challenges in cybersecurity.[66]

Key New Hampshire State and Federal Government Cyber Entities

Local, state, and federal government agencies have a vital role in protecting residents from cyberattacks and bringing cybercriminals that attack Americans to justice. Third Way has compiled a list of these entities:

State Cyber Entities

- **New Hampshire Cyber Integration Center (NHCIC):** The NHCIC serves as New Hampshire's focal point for coordinating cybersecurity monitoring, information sharing, and threat analysis.[67]
- **New Hampshire Information and Analysis Center (NHIAC):** The NHIAC serves as New Hampshire's all-crimes/all-hazards information and analysis center. It can monitor open and classified sources, including those related to cyber threats, and then share information with the public and private sector.[68]
- **New Hampshire Department of Safety:** The Department of Safety operates the cybersecurity alert level to allow the public to monitor daily levels of malicious cyber activity.[69] It also houses the state's homeland security and emergency operations, which have the responsibility of responding to major disasters.[70]
- **New Hampshire Department of Information Technology:** The Department of Information Technology serves as a unified government entity for all of New Hampshire's cyber resources. The Department of Information Technology is led by a Commissioner and has legal authority to manage and coordinate all technology resources for the state government.[71]
- **New Hampshire Department of Safety:** The Department of Safety contains the Major Crimes Unit within the Investigative Services Bureau, which has computer crime investigators that handle many of New Hampshire's cybercrime investigations.[72]

Federal Cyber Entities

There are not many federal law enforcement agencies with field offices in New Hampshire. The only notable entity is a US Attorney's Office located in Concord, New Hampshire:

- **US Attorney's Office for the District of Hampshire:** The US Attorney's Office serves as the state's chief federal law enforcement officer and prosecutes cybercrimes within New Hampshire.[73]

University Cyber Centers

To effectively address cyberattacks, local, state, and federal entities need trained cyber professionals. There are 299,000 unfilled cybersecurity positions in the United States and the gap is expected to reach 1.8 million by 2022, according to a 2018 report authored jointly by the

Department of Commerce and DHS.[74] The gap in unfilled cybersecurity positions covers both the private and public sector, and vacancies range from IT specialists to law enforcement cyber investigators. The large vacancy in positions affects the government and companies' abilities to improve their cybersecurity and law enforcement's ability to go after cybercriminals.[75] Universities are taking a lead in addressing this cyber workforce shortage and are creating cyber centers to provide education and training resources for the next generation of cyber professionals.

Here is a list of New Hampshire universities that have created cyber centers:

- **Dartmouth College, Institute for Security Technology, and Society:** Has been designated a Center of Academic Excellence in Information Research by the National Security Agency and DHS. Its mission is to research and advance information security and privacy.[76]
- **University of New Hampshire Cybersecurity Center of Excellence:** The Cyber Center partners with academia, industry, and government. Its mission is to educate cybersecurity professionals on technical and societal challenges in cybersecurity.[77]

Military Installations in New Hampshire

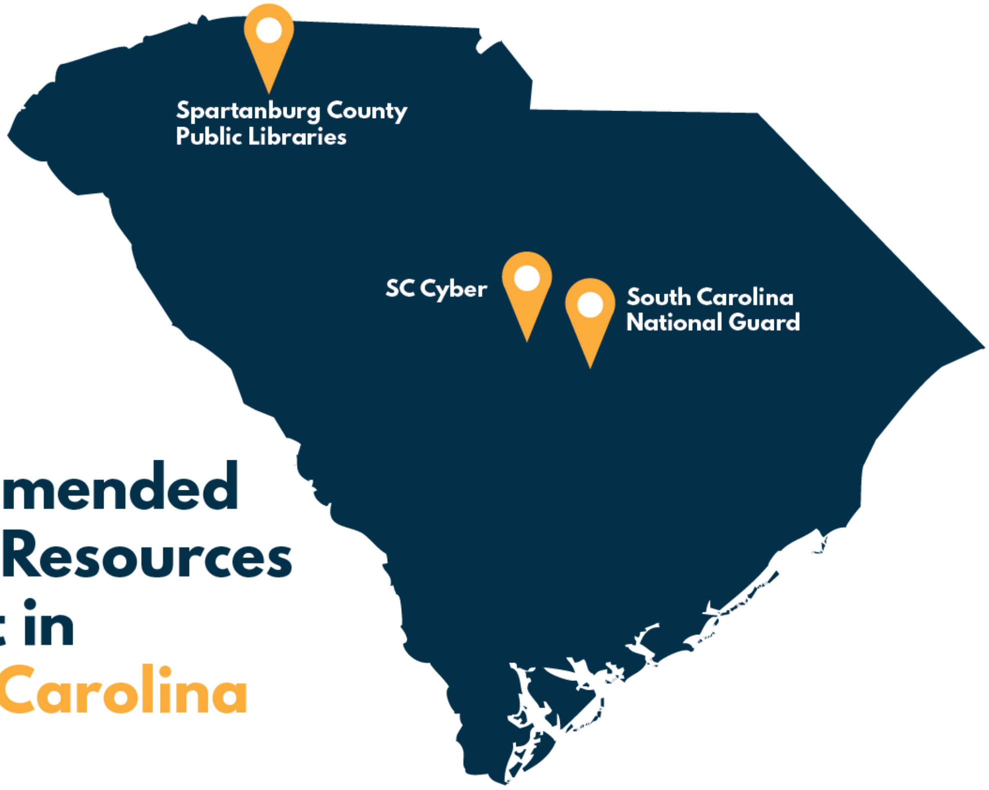
States are using their National Guard units to combat the growing national security threat of cyberattacks. National Guard units are being organized into cyber mission teams. Some are tasked with protecting state-level interests, and others are under the direction of US Cyber Command and are charged with protecting Department of Defense networks and national critical infrastructure.[78] There are currently 3,880 National Guardsmen assigned to cyber service, spread across 59 cyber units in 38 states.[79]

Here are all the major military installations in New Hampshire:

- Portsmouth Shipyard, Portsmouth, NH
- Pease Air National Guard, Portsmouth, NH
- United States Coast Guard Station Portsmouth Harbor, New Castle, NH
- United States Army Cold Regions Research and Engineering Laboratory, Hanover, NH
- Army National Guard, Nashua, NH
- Army National Guard, Rochester, NH

Cyber Resources: South Carolina

THIRD WAY


Spartanburg County Public Libraries
SC Cyber
South Carolina National Guard

Recommended Cyber Resources to Visit in South Carolina

Overview of South Carolina's Cyber Response

In 2016 and 2017, over 3,500 South Carolinians reported internet crime complaints to the FBI.[80] The financial impact of cyberattacks on South Carolina continues to increase. In 2016, South Carolinians reported a loss close to $11 million[81] and in 2017 over $13 million[82] to the FBI due to cybercrime.[83]

In response to the growing cyber threat, South Carolina General Assembly created the Division of Information Security in 2013, giving it responsibility for statewide polices, standards, and coordination of cybersecurity resources.[84]

As many states mobilize their cyber resources, here are three unique measures South Carolina has developed to improve its ability to respond to cyberattacks:

- **Created cyber education programs:** The University of South Carolina and the South Carolina Department of Commerce founded SC Cyber in 2016.[85] SC Cyber partners with academia, industry, and government to create and offer programs related to cyber training, workforce development, education, advanced technology development, and critical infrastructure protection.[86]

- **Modernized cybersecurity legislation:** South Carolina passed new cybersecurity laws for insurance companies licensed in the state effective January 1, 2019.[87] The rules require licensed insurance companies to notify state insurance authorities of data breaches within 72 hours after confirming that nonpublic data within the insurance company's system was accessed.[88]
- **Instituted a centralized management system for cyber:** South Carolina has organized the states' information technology into a Division of Information Security led by a Chief Information Security Officer.[89] It is important for states to have a centralized manager who can mobilize and coordinate resources during a cyber incident.

Examples of Recent South Carolina Cyberattacks

Cyberattacks have hit every sector of the US economy. Here are recent examples of the impact cyberattacks have had on local municipalities and businesses in South Carolina:

Government

- In January 2018, the Spartanburg County Public Libraries were the target of a ransomware attack, an attack that prevents users from accessing their computer system until a payment is made. The county has a population close to 300,000.[90] The cybercriminals blocked access to the computer system unless $36,000 in bitcoin was paid. The attack halted all access to the Libraries online catalog and website.[91]
- In December 2018, the Mount Pleasant Police Department's computer system was infected with ransomware. The department was able to remove the infected computers from the networks before the cyberattack caused more severe damage.[92]

Medical

- In November 2018, employees at Roper St. Francis were hit with a phishing attack, allowing malicious actor to gain access to their email accounts. The cybercriminal was able to gain access to some patient information such as medical record numbers health insurance information, and some Social Security numbers.[93]

Education

- In January 2019, hackers infiltrated the computer network of Greenwood School District 5 and stole $1,200 by accessing the payroll system.[94]

Recommended Cyber Resources to Visit

Third Way has identified three vital stops in South Carolina. One stop was the victim of a cyberattack and showcases how malicious cyber activity has impacted South Carolina. The other two stops are measures South Carolina is taking to protect residents and critical infrastructure from the cyber threat:

- **SC Cyber:** is based at the University of South Carolina, SC Cyber is a consortium of partners across academia, industry, and government. The mission of this entity is to provide cyber training, education, workforce development, advanced technology development, and critical infrastructure protection.[95]

- **Spartanburg County Public Libraries:** in January 2018, the Spartanburg County Public Libraries were the target of a ransomware attack. The cybercriminals blocked access to the computer system unless $36,000 in bitcoin was paid. The attack halted all access to the Libraries online catalog and website.[96]
- **South Carolina National Guard:** works to protect the state against cyberattacks through the 125th Cyber Protection Battalion, which was established in 2017 by South Carolina as the first unit assigned to protect the state against cyberattacks.[97]

Key South Carolina State and Federal Government Cyber Entities

Local, state, and federal government agencies have a vital role in protecting residents from cyberattacks and bringing to justice cybercriminals that attack Americans. Third Way has compiled a list of government entities:

State Cyber Entities

- **South Carolina, Law Enforcement Division (SLED):** The SLED is the statewide law enforcement agency.
  - The Computer Crime Center works to investigative cybercrimes in the state.[98]
  - The Homeland Security division responds to any emergency incident in the state including those that are cyber-related.[99]
- **SC Cyber:** SC Cyber is based at the University of South Carolina and is a consortium of partners across academia, industry, and government. The mission is to provide cyber training, education, workforce development, advanced technology development, and critical infrastructure protection.[100]
- **Division of Information Security:** The Division of Information Security is led by the South Carolina Chief Information Officer and is responsible for setting statewide cyber polices standards, programs, and services.[101]
- **South Carolina InfraGard:** InfraGard is an information sharing partnership between the FBI and the private sector in South Carolina designed to protect critical infrastructure.[102]
- **South Carolina National Guard:** The South Carolina National Guard established the 125th Cyber Protection Battalion, the first unit assigned to protect the state against cyberattacks.[103]

Federal Cyber Entities

- **Federal Bureau of Investigation:** The FBI maintains a field office in Columba, SC. [104]
- **US Attorney's Office for the District of South Carolina:** The US Attorney's Office is the chief federal law enforcement officer in the state and has offices in Columbia, Greenville, Florence, and Charleston. Through the Criminal Division, the Office prosecutes cybercrimes within the state of South Carolina.[105]
- **United States Secret Service (USSS):** The USSS operates a South Carolina Electronic Crimes Task Force designed to prevent, detect, and investigate cyberattacks on financial institutions and critical infrastructures.[106]

University Cyber Centers

To effectively address cyberattacks, local, state, and federal entities need trained cyber professionals. There are 299,000 unfilled cybersecurity positions in the United States and the gap is expected to reach 1.8 million by 2022, according to a 2018 report authored jointly by the Department of Commerce and DHS.[107] The gap in unfilled cybersecurity positions covers both the private and public sectors and vacancies range from IT specialists to law enforcement cyber investigators. The large vacancy in positions affects the government and companies' ability to improve their cybersecurity and law enforcement's ability to go after cybercriminals.[108] Universities are taking a lead in addressing this cyber workforce shortage and are creating cyber centers to provide education and training resources for the next generation of cyber professionals.

Here is a list of South Carolina universities that have created cyber centers:

- **Clemson University Cybersecurity Center:** The Cybersecurity Center engages in cybersecurity research, education, industry partnership, and community engagement.[109]
- **SC Cyber:** SC Cyber is based at the University of South Carolina and is a consortium of partners across academia, industry, and government. The mission is to provide cyber training, education, workforce development, advanced technology development, and critical infrastructure protection.[110]
- **South Carolina State University Center for Excellence in Cyber Security:** The Center for Excellence is designed to serve as a focal point on cyber education, training, and awareness.[111]
- **Trident Technical College Cyber Center:** The Cyber Center is the recipient of an Office of Naval Research grant until 2020, and its goal is to promote higher education and research in cyber defense and training professionals with cyber defense expertise.[112]

Military Installations in South Carolina

States are using their National Guard units to combat the growing national security threat of cyberattacks. National Guard units are being organized into cyber mission teams. Some are tasked with protecting state-level interests, and others are under the direction of US Cyber Command and are charged with protecting Department of Defense networks and national critical infrastructure.[113] There are currently 3,880 National Guardsmen assigned to cyber service, spread across 59 cyber units in 38 states.[114]

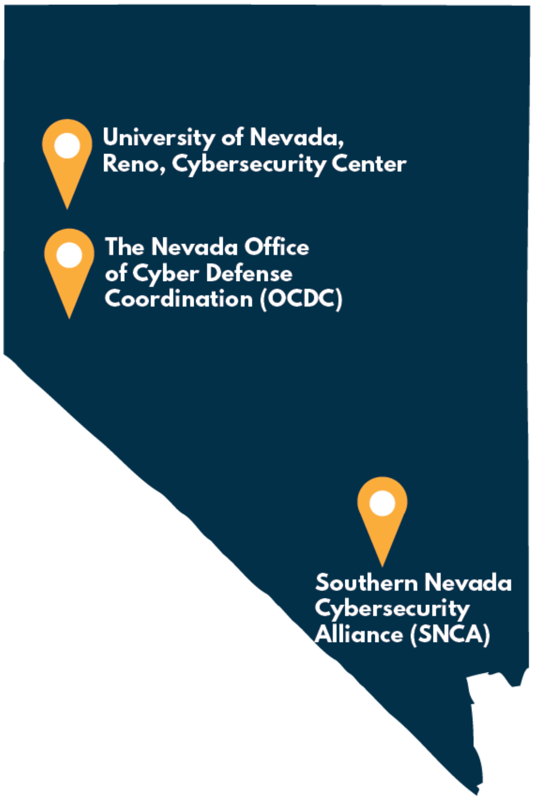
Here are all the major military installations in South Carolina:

- Fort Jackson, Columbia, SC
- Marine Corps Air Station Beaufort, Beaufort, SC
- Marine Crops Recruit Depot Parris Island, Port Royal, SC
- Naval Hospital Beaufort, Beaufort, SC
- Naval Hospital Charleston, Charleston, SC
- Naval Weapons Station Charleston, Goose Creek, SC

Cyber Resources: Nevada

THIRD WAY

Recommended Cyber Resources to Visit in Nevada


University of Nevada, Reno, Cybersecurity Center
The Nevada Office of Cyber Defense Coordination (OCDC)
Southern Nevada Cybersecurity Alliance (SNCA)

Overview of Nevada's Cyber Response

In 2016, Nevadans filed over 3,700[115] internet crime complaints to the FBI, and the figure ballooned to over 4,600 in 2017.[116] The economic impact of these crimes has continued to increase. In 2016 Nevadans reported a financial loss of over $15 million,[117] which increased in 2017 to over $19 million.[118]

In response to the growing cyber threat, Nevada passed legislation to establish the Nevada Office of Cyber Defense Coordination (OCDC) in 2017. It was designed to integrate state cyber resources and oversee implementation of Nevada's cybersecurity strategy. It is responsible for policy, planning, and coordination in the event of a cyber incident.[119]

As many states mobilize their cyber resources, here are three unique measures Nevada developed to improve its ability to respond to cyberattacks:

- **Established grants to train cyber professionals:** Nevada views cybersecurity professionals as vital to its economy. The Nevada Governor's Office of Science, Innovation, and Technology has awarded over $600,000 in grants to organizations create cyber workforce programs.[120] Nevada has as many as 1,6333 unfilled cybersecurity job openings.[121]

- **Formed private and public sector cyber incident response organizations:** Southern Nevada Cybersecurity Alliance is a volunteer service of cybersecurity professionals, who responded to cyber incidents threatening the critical infrastructure of Las Vegas, North Las Vegas, and Henderson.[122]
- **Started cyber initiatives to empower students and women:** In February 2019, Nevada Governor Steve Sisolak announced that Nevada is partnering with other organizations to launch Girls Go Cyberstart and Cyber FastTrack. These two initiatives to help young women in high school and college with opportunities to gain cybersecurity skills and help with professional development.[123]

Examples of Recent Nevada Cyberattacks

Cyberattacks have hit every sector of the US economy. Here are recent examples of the impact cyberattacks have had on local municipalities and businesses in Nevada:

Government

In 2016, the Nevada Department of Transportation was hit by a cyberattack, compromising the Personal Indefinable Information of state employees, such as dates of birth and Social Security numbers.[124]

Business

- In 2016, a cyberattack against the Nevada State Medical Marijuana Program led to the records of medical marijuana card holders being leaked.[125]
- In 2016, the Hard Rock Las Vegas suffered its second data breach, with malware targeting the credit card information of customers.[126]
- In 2014, the Las Vegas Sands casino was the victim of an Iranian cyberattack, which crippled thousands of servers by wiping them with malware.[127]
- In 2014, the Venetian and Palazzo casinos websites were hacked. The casino websites were taken down and employee personal information was stolen, costing almost $40 million in damage.[128]

Recommended Cyber Resources to Visit

Third Way has identified three vital state resources that showcase measures Nevada is taking to protect residents and critical infrastructure from the national security threat of cyberattacks:

- **University of Nevada, Reno, Cybersecurity Center:** The Cybersecurity Center focuses on educational and research opportunities in cybersecurity and seeks to enhance Nevada's cybersecurity readiness.[129]
- **The Nevada Office of Cyber Defense Coordination (OCDC):** OCDC serves as Nevada's centralized hub for cybersecurity strategy, planning, and coordination.[130]
- **Southern Nevada Cybersecurity Alliance (SNCA):** SNCA is a volunteer service of cybersecurity professionals committed to defending the critical infrastructure of Las Vegas, North Las Vegas, and Henderson Nevada from cyberattacks.[131]

Key Nevada State and Federal Government Cyber Entities

Local, state, and federal government agencies have a vital role in protecting residents from cyberattacks and they have the authority to go after cybercriminals. Third Way has compiled a list of these agencies:

State Cyber Entities

The Nevada Office of Cyber Defense Coordination (OCDC): OCDC serves as Nevada's centralized hub for cybersecurity strategy, planning, and coordination.[132]

- **Department of Emergency Management, Homeland Security Section (DEM):** The Homeland Security Section mobilizes state resources to respond to acts of terrorism and related emergency, including cyber incidents.[133]
- **Department of Business and Industry, Nevada Consumer Affairs:** The Office of Consumer Affairs works to protect residents from unfair and deceptive business practices, including online scams.[134]
- **Attorney General:** The Attorney General operates a Technological Crime Advisory Board, consisting of state, local, and federal officers, designed to facilitate cooperation in the detection, investigation, and prosecution of technological crimes.[135]

Federal Cyber Entities

US Attorney's Office for the District of Nevada: The US Attorney's Office comprises the entire state of Nevada. Through its Criminal Division, it can prosecute any cybercrime in the state.[136]

- **Federal Bureau of Investigation:** The FBI maintains a field office in Las Vegas.[137]
- **Homeland Security Investigations (HSI):** HSI operates a field office in Las Vegas.[138]
- **United States Secret Service (USSS):** USSS operates a field office in Reno and Las Vegas.[139]

University Cyber Centers

To effectively address cyberattacks, local, state, and federal entities need trained cyber professionals. There are 299,000 unfilled cybersecurity positions in the United States and the gap is expected to reach 1.8 million by 2022, according to a 2018 report authored jointly by the Department of Commerce and DHS.[140] The gap in unfilled cybersecurity positions covers both the private and public sectors and vacancies range from IT specialists to law enforcement cyber investigators. The large vacancy in positions affects the government and companies' ability to improve their cybersecurity and law enforcement's ability to go after cybercriminals.[141] Universities are taking a lead in addressing this cyber workforce shortage and are creating cyber centers to provide education and training resources for the next generation of cyber professionals.

Here is a list of Nevada universities that have created cyber centers:

- **University of Nevada, Reno's Cybersecurity Center:** The Cybersecurity Center focuses on educational and research opportunities in cybersecurity and seeks to enhance Nevada's cybersecurity readiness.[142]

- **University of Nevada, Las Vegas, Cybersecurity Center:** The Center is focused on educating and training cyber professionals in cyber defense to address the cybersecurity workforce shortage.[143]

Military Installations in Nevada

States are using their National Guard units to combat the growing national security threat of cyberattacks. National Guard units are being organized into cyber mission teams. Some are tasked with protecting state-level interests, and others are under the direction of US Cyber Command and are charged with protecting Department of Defense networks and national critical infrastructure.[144] There are currently 3,880 National Guardsmen assigned to cyber service, spread across 59 cyber units in 38 states.[145]

Here are all the major military installations in Nevada:

- Naval Air Station Fallon, Fallon, NV
- Nevada Army National Guard, Carson City, NV
- Nevada Army National Guard, Clark County Army, Las Vegas, NV
- Creech Air Force Base, Indian Springs, NV
- Nevada National Guard, Reno, NV
- Naval Undersea Warfare, Hawthorne NV
- Nellis Air Force Base, Nellis AFB, NV

Appendix A

To Catch a Hacker: Third Way Policy Recommendations

Cybercriminals operate with a sense of impunity as only 0.3% of malicious cyber incidents see an arrest, according to our analysis of FBI reported data. What that means is that the United States is facing a massive cyber enforcement gap just as the cybercrime wave continues and malicious cyber activity that threatens our national security is becoming more common.

Domestic Enforcement Reform

1. **A Larger Role for Law Enforcement:** Strengthen capacity building efforts so that law enforcement, enabled by diplomacy, can target the humans behind cyberattacks.
2. **A Cyber Enforcement Cadre:** Address not only workforce shortages, but the way the cyber enforcement workforce is trained, incentivized, and retained.
3. **Better Attribution Efforts:** Increase investments in research and development for attribution technology, better digital forensics, and prioritize efforts to build international alliances that improve timeliness and impact of attribution efforts.
4. **A Carrot and Stick Approach to Fugitives:** Adopt a broader reward-based system to incentivize information sharing that can lead to arrests of malicious cyber actors balanced with the smart use of targeted sanctions.

International Cooperation and Coordination Reform

5. **An Ambassador-level Cyber Quarterback:** Institute an ambassador-level cyber coordinator position at the State Department with a clear mandate and resources on cyber enforcement.
6. **Stronger Tools in the Diplomacy Arsenal:** Expand the number and streamline processes for agreements with other countries that help bring cyber attackers to justice and continue to utilize the multilateral Budapest Convention.
7. **Better International Capacity for Enforcement:** Support efforts to build the capacity of other countries on cybercrime investigations, while ensuring cybercrime and cybersecurity efforts are not used to suppress civil liberties and human rights.

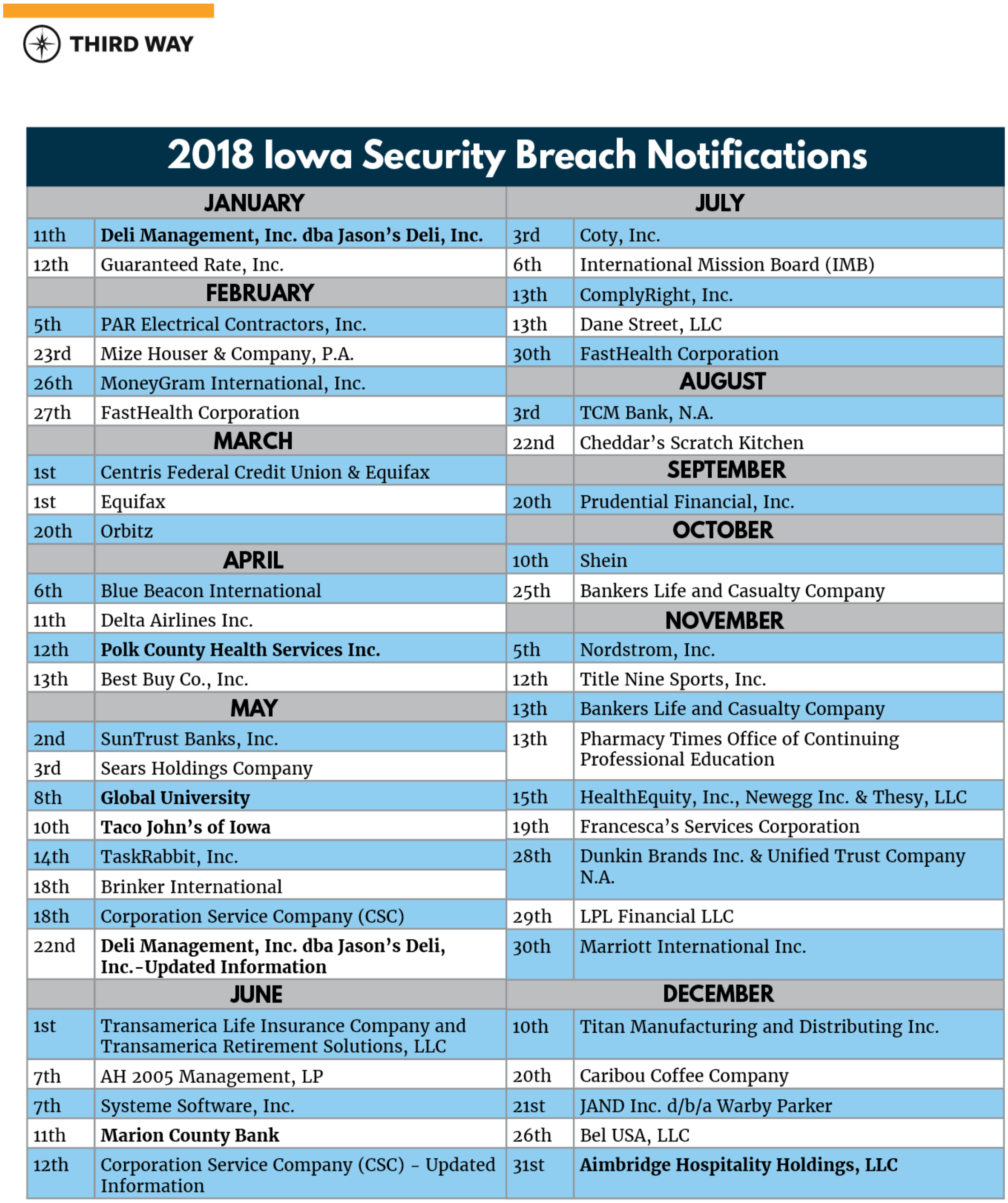
Structural and Process Reform

8. **Better Success Metrics:** Establish mechanisms to measure the scope of the cyber enforcement problem and the effectiveness of government efforts.
9. **Organizational Changes and Interagency Cooperation:** Evaluate further needed policy changes to de-conflict the missions of the agencies responsible for cyber enforcement.
10. **Centralized Strategic Planning:** Institute an overarching, comprehensive strategy for US cyber enforcement led by a senior official at the White House.

Appendix B

Iowa Data Breach Notifications

The Iowa Attorney General maintains a database online of all security breach notifications in the state since 2011. Iowa law requires anyone that encounters a security breach that affects at least 500 Iowa residents to report the breach within five business days after notifying affected people to the Attorney General's Consumer Protection Division Director. The below chart is those companies that reported data breaches to the Iowa Attorney General in the year 2018. Companies bolded are local Iowa businesses.



THIRD WAY

2018 Iowa Security Breach Notifications

	JANUARY		**JULY**
11th	**Deli Management, Inc. dba Jason's Deli, Inc.**	3rd	Coty, Inc.
12th	Guaranteed Rate, Inc.	6th	International Mission Board (IMB)
	FEBRUARY	13th	ComplyRight, Inc.
5th	PAR Electrical Contractors, Inc.	13th	Dane Street, LLC
23rd	Mize Houser & Company, P.A.	30th	FastHealth Corporation
26th	MoneyGram International, Inc.		**AUGUST**
27th	FastHealth Corporation	3rd	TCM Bank, N.A.
	MARCH	22nd	Cheddar's Scratch Kitchen
1st	Centris Federal Credit Union & Equifax		**SEPTEMBER**
1st	Equifax	20th	Prudential Financial, Inc.
20th	Orbitz		**OCTOBER**
	APRIL	10th	Shein
6th	Blue Beacon International	25th	Bankers Life and Casualty Company
11th	Delta Airlines Inc.		**NOVEMBER**
12th	**Polk County Health Services Inc.**	5th	Nordstrom, Inc.
13th	Best Buy Co., Inc.	12th	Title Nine Sports, Inc.
	MAY	13th	Bankers Life and Casualty Company
2nd	SunTrust Banks, Inc.	13th	Pharmacy Times Office of Continuing Professional Education
3rd	Sears Holdings Company		
8th	**Global University**	15th	HealthEquity, Inc., Newegg Inc. & Thesy, LLC
10th	**Taco John's of Iowa**	19th	Francesca's Services Corporation
14th	TaskRabbit, Inc.	28th	Dunkin Brands Inc. & Unified Trust Company N.A.
18th	Brinker International		
18th	Corporation Service Company (CSC)	29th	LPL Financial LLC
22nd	**Deli Management, Inc. dba Jason's Deli, Inc.-Updated Information**	30th	Marriott International Inc.
	JUNE		**DECEMBER**
1st	Transamerica Life Insurance Company and Transamerica Retirement Solutions, LLC	10th	Titan Manufacturing and Distributing Inc.
7th	AH 2005 Management, LP	20th	Caribou Coffee Company
7th	Systeme Software, Inc.	21st	JAND Inc. d/b/a Warby Parker
11th	**Marion County Bank**	26th	Bel USA, LLC
12th	Corporation Service Company (CSC) – Updated Information	31st	**Aimbridge Hospitality Holdings, LLC**

ENDNOTES

[1] Poushter, Jacob, and Christine Huang. "Climate Change Still Seen as Top Global Threat, but Cyberattacks Rising Concern." Pew Research Center's Global Attitudes Project, Pew Research Center, 11 Feb. 2019, www.pewglobal.org/2019/02/10/climate-change-still-seen-as-the-top-global-threat-but-cyberattacks-a-rising-concern/. Accessed 11 April 2019.

[2] The Cost of Malicious Cyber Activity to the U.S. Economy. The Council of Economic Advisers, Feb. 2018, www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 15 April 2019.

[3] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[4] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 15 April 2019.

[5] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 15 April 2019.

[6] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[7] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[8] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[9] A copy of the 10 areas of recommendations made in the report can be found in Appendix A.

[10] https://pdf.ic3.gov/2017_IC3Report.pdf

[11] Office of Financial Research. "2017 Annual Report to Congress." 29 Sept. 2017, pp. 6. https://www.financialresearch.gov/annual-reports/files/office-of-financial-research-annual-report-2017.pdf. Accessed Oct. 3, 2018.

[12] Gaskew, Brandon. "Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget –Third Way." Third Way, Third Way, 21 Feb. 2019, https://www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget. Accessed 15 April 2019.

[13] "Clearances." ***FBI***, Federal Bureau of Investigation, 25 Aug. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/clearances. Accessed 19 Oct. 2018.

[14] Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 19. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 16 April 2019.

[15] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 22 https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[16] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 23. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[17] These figures do not necessarily provide a complete picture of Iowans' economic losses because many cybercrime victims do not report their victimization to law enforcement. Source: Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New

York Times, 5 Mar. 2018, http://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 16 April 2019.

18 “State of Iowa Cybersecurity Strategy.” Information Security Division, Office of the Chief Information Officer, 5 Aug. 2016, ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf. Accessed 16 April 2019.

19 “State of Iowa Cybersecurity Strategy.” Information Security Division, Office of the Chief Information Officer, 5 Aug. 2016, ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf. Accessed 16 April 2019.

20 “Iowa Cyber Alliance.” Information Assurance Center, Iowa State University, 10 Jan. 2017, www.iac.iastate.edu/iowa-cyber-alliance/. Accessed 16 April 2019.

21 “State of Iowa Cybersecurity Strategy.” Information Security Division, Office of the Chief Information Officer, 5 Aug. 2016, ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf. Accessed 16 April 2019.

22 “Cybersecurity.” Cybersecurity, Safeguard Iowa Partnership, www.safeguardiowa.org/cybersecurity. Accessed 16 April 2019.

23 “What We Do.” Office of the Chief Information Officer, Office of the Chief Information Officer, ocio.iowa.gov/about-us/what-we-do. Accessed 16 April 2019.

24 “Security Breach Notifications.” Iowa Attorney General, Iowa Attorney General, www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/. Accessed 22 April 2019.

25 Appendix B contains a full list of all 2018 company data breach notifications reported to the Iowa AG.

26 Ecklund, Meredith. “Muscatine Cyber Attack Affects More than City.” Muscatine Journal, Muscatine Journal, 22 Oct. 2018, muscatinejournal.com/muscatine/news/local/muscatine-cyber-attack-affects-more-than-city/article_91f81f8c-e5db-56bc-a082-44c5a698ada9.html. Accessed 22 April 2019.

27 “Muscatine Cyber Attack Targets Government Financial Server.” WQAD.com, WQAD8, 19 Oct. 2018, wqad.com/2018/10/19/muscatine-cyber-attack-targets-government-financial-server/. Accessed 22 April 2019.

28 Ransomware is a type of malicious software (malware) that prevents users from accessing their system or a part of it until a ransom is paid (to the attacker).

29 “Muscatine Cyber Attack Targets Government Financial Server.” WQAD.com, WQAD8, 19 Oct. 2018, wqad.com/2018/10/19/muscatine-cyber-attack-targets-government-financial-server/. Accessed 22 April 2019.

30 Donovan, Fred. “Ransomware Attack at Iowa Eye Clinic Puts PHI of 40K at Risk.” HealthITSecurity, HealthITSecurity, 1 Nov. 2018, healthitsecurity.com/news/ransomware-attack-at-iowa-eye-clinic-puts-phi-of-40k-at-risk. Accessed 22 April 2019.

31 Leys, Tony. “UnityPoint Warns 1.4 Million Patients Their Information Might Have Been Breached by Email Hackers.” Des Moines Register, Des Moines Register, 30 July 2018, www.desmoinesregister.com/story/news/health/2018/07/30/unitypoint-data-breach-million-patients-email-hack-hacked-phishing-e-mail-health-care-iowa/866760002/. Accessed 22 April 2019.

32 Ta, Linh, and Jason Clayworth. “‘Dark Overlord’ Hackers Posted Stolen Student Info, Johnston Officials Say.” Des Moines Register, Des Moines Register, 5 Oct. 2017, www.desmoinesregister.com/story/news/crime-and-courts/2017/10/05/dark-overlord-hacker-johnston-schools-threats/735950001/. Accessed 22 April 2019.

33 “Iowa Cyber Alliance.” Information Assurance Center, Iowa State University, 10 Jan. 2017, www.iac.iastate.edu/iowa-cyber-alliance/. Accessed 22 April 2019.

34 “State of Iowa Cybersecurity Strategy.” Information Security Division, Office of the Chief Information Officer, 5 Aug. 2016, ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf. Accessed 22 April 2019.

35 Kelly, Michael J. “132d Wing Activates New Cyberspace Operations Squadron.” 132d Wing, United States Air Force, 6 Nov. 2017, www.132dwing.ang.af.mil/News/Article-Display/Article/1363646/132d-wing-activates-new-cyberspace-operations-squadron/. Accessed 22 April 2019.

36 “Muscatine Government Cyber Attack Recovery ‘a Slow Process’.” WQAD.com, WQAD8, 2 Nov. 2018, wqad.com/2018/11/02/muscatine-government-cyber-attack-recovery-a-slow-process/. Accessed 22 April 2019.

37 “What We Do.” Office of the Chief Information Officer, Office of the Chief Information Officer, ocio.iowa.gov/about-us/what-we-do. Accessed 22 April 2019.

38 “About.” Office of the Chief Information Officer, Office of the Chief Information Officer, https://iso.iowa.gov/about-our-vision-mission. Accessed 22 April 2019.

39 “IOWA DIVISION OF CRIMINAL INVESTIGATION FIELD OPERATIONS BUREAU CYBER-CRIME UNIT.” Cyber Crime Unit, Iowa Department of Public Safety, www.dps.state.ia.us/DCI/fieldoperations/cybercrime.shtml. Accessed 22 April 2019.

40 “Incident Response.” Icn.iowa.gov, Iowa Communication Network, icn.iowa.gov/services/incident-response. Accessed 22 April 2019.

41 “Department Overview.” Iowa Homeland Security and Emergency Management, Iowa Homeland Security and Emergency Management , www.homelandsecurity.iowa.gov/about_HSEMD/department_overview.html. Accessed 22 April 2019.

42 “2019 Security Breach Notifications.” Iowa Attorney General, Iowa Attorney General, www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/2019/. Accessed 22 April 2019.

43 “State of Iowa Cybersecurity Strategy.” Information Security Division, Office of the Chief Information Officer, 5 Aug. 2016, ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf. Accessed 22 April 2019.

44 “Divisions.” The United States Department of Justice, The United States Attorney’s Office Southern District of Iowa, 18 Apr. 2019, www.justice.gov/usao-sdia/divisions. Accessed 22 April 2019.

45 “Divisions.” The United States Department of Justice, The United States Attorney’s Office Northern District of Iowa, 10 July 2018, www.justice.gov/usao-ndia/divisions. Accessed 22 April 2019.

46 Eoyang, Mieke, et al. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

47 Eoyang, Mieke, et al. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

48 “EICC Cyber Center.” EICC Cyber Center, Eastern Iowa Community College, www.eicc.edu/cybersecurity. Accessed 22 April 2019,

49 “Iowa CyberHub.” Iowa Cyber Hub, Iowa State University and Des Moines Area Community College, www.iowacyberhub.org/Pages/welcome.aspx. Accessed 22 April 2019.

50 “Information Assurance Center.” Information Assurance Center, Iowa State University, www.iac.iastate.edu/. Accessed 22 April 2019.

51 Maucione, Scott. “Natl’ Guard Cyber Units Protect Country’s Interests, Still Face Training Issues.” Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

52 Maucione, Scott. “Natl’ Guard Cyber Units Protect Country’s Interests, Still Face Training Issues.” Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

[53] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 23. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[54] Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 19. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 16 April 2019.

[55] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 22. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[56] These figures do not necessarily provide a complete picture of New Hampshirites' economic losses because many cybercrime victims do not report their victimization to law enforcement. Source: Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New York Times, 5 Mar. 2018, http://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 16 April 2019.

[57] "New Hampshire Cyber Integration Center." Department of Information Technology, Department of Information Technology, www.nh.gov/doit/cybersecurity/nh-cic/index.htm. Accessed 22 April 2019.

[58] "Cyber Security Alert Level." Cyber Alert Level, Department of Information Technology and Department of Safety, www.nh.gov/safety/infotech/cyberalert.html. Accessed 22 April 2019.

[59] "New Hampshire Cyber Integration Center." Department of Information Technology, Department of Information Technology, www.nh.gov/doit/cybersecurity/nh-cic/index.htm. Accessed 22 April 2019.

[60] Polsen, Jim. "Cyberattack May Have Affected Some New England Utility Customers." Bloomberg.com, Bloomberg, 6 Apr. 2018, www.bloomberg.com/news/articles/2018-04-06/cyberattack-may-have-affected-some-new-england-utility-customers. Accessed 22 April 2019.

[61] Dinan, Elizabeth. "Portsmouth Warning: Phony Bills Emailed to Residents." Seacoastonline.com, The Portsmouth Herald, 30 Mar. 2018, www.seacoastonline.com/news/20180329/portsmouth-warning-phony-bills-emailed-to-residents. Accessed 22 April 2019.

[62] "Manchester, N.H., Firm Hit by Cyberattack, Disrupting Internet across East Coast." The Eagle Tribune, The Eagle Tribune, 21 Oct. 2016, www.eagletribune.com/news/manchester-n-h-firm-hit-by-cyberattack-distrupting-internet-across/article_8dc06f14-979a-11e6-ae91-8fbd4a94169c.html. Accessed 22 April 2019.

[63] Schinella, Tony. "Concord School District Reports 'Data Security Breach'." Concord, NH Patch, Patch, 3 June 2016, patch.com/new-hampshire/concord-nh/concord-school-district-reports-data-security-breach-0. Accessed 22 April 2019.

[64] "New Hampshire Cyber Integration Center." Department of Information Technology, Department of Information Technology, www.nh.gov/doit/cybersecurity/nh-cic/index.htm. Accessed 22 April 2019.

[65] "Investigative Services Bureau: Major Crimes Unit." Division of State Police, New Hampshire Department of Public Safety, www.nh.gov/safety/divisions/nhsp/isb/majorcrime/index.html. Accessed 22 April 2019.

[66] "UNH CYBERSECURITY CENTER OF EXCELLENCE." College of Engineering and Physical Sciences, University of New Hampshire, 18 Jan. 2019, ceps.unh.edu/cyber. Accessed 22 April 2019.

[67] "New Hampshire Cyber Integration Center." New Hampshire Cyber Integration Center, Department of Information Technology, www.nh.gov/doit/cybersecurity/nh-cic/index.htm. Accessed 22 April 2019.

[68] "Welcome to the New Hampshire Information and Analysis Center." New Hampshire Information and Analysis Center, New Hampshire Department of Public Safety, https://www.nh.gov/safety/information-analysis-center/. Accessed 22 April 2019.

[69] "Cyber Security Alert Level." Cyber Alert Level, Department of Information Technology and Department of Safety, www.nh.gov/safety/infotech/cyberalert.html. Accessed 22 April 2019.

[70] "Welcome!" Homeland Security & Emergency Management, New Hampshire Department of Public Safety, www.nh.gov/safety/divisions/hsem/index.html. Accessed 22 April 2019.

[71] "New Hampshire Cyber Integration Center." Department of Information Technology, Department of Information Technology, www.nh.gov/doit/cybersecurity/nh-cic/index.htm. Accessed 22 April 2019.

[72] "Investigative Services Bureau: Major Crimes Unit." Division of State Police, New Hampshire Department of Public Safety, www.nh.gov/safety/divisions/nhsp/isb/majorcrime/index.html. Accessed 22 April 2019.

[73] "District of New Hampshire." The United States Department of Justice, The United States Attorney's Office District of New Hampshire, 9 Nov. 2018, www.justice.gov/usao-nh. Accessed 22 April 2019.

[74] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[75] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[76] "About ISTS." ISTS, Dartmouth College Center of Academic Excellence in Information Assurance Research, www.ists.dartmouth.edu/about/. Accessed 23 April 2019.

[77] "UNH CYBERSECURITY CENTER OF EXCELLENCE." College of Engineering and Physical Sciences, University of New Hampshire, 18 Jan. 2019, ceps.unh.edu/cyber. Accessed 23 April 2019.

[78] Maucione, Scott. "Natl' Guard Cyber Units Protect Country's Interests, Still Face Training Issues." Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

[79] Maucione, Scott. "Natl' Guard Cyber Units Protect Country's Interests, Still Face Training Issues." Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

[80] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 23. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[81] Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 19. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 16 April 2019.

[82] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 22. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[83] These figures do not necessarily provide a complete picture of South Carolinians' economic losses because many cybercrime victims do not report their victimization to law enforcement. Source: Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New York Times, 5 Mar. 2018, http://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 16 April 2019.

[84] "About Information Security." About Information Security | Department of Administration State of South Carolina, Department of Administration State of South Carolina, www.admin.sc.gov/technology/information-security/about-information-security. Accessed 23 April 2019.

[85] "SC Cyber." Fiscal Year 2018 Annual Report, SC Cyber, cdn.ymaws.com/www.sccyber.org/resource/collection/D684A6A7-E0B8-45C2-939A-BBA5320F7DE6/20180805_-_SC_Cyber_Annual_Report_2017-2018_FINAL.pdf. Accessed 23 April 2019.

[86] "SC Cyber." Fiscal Year 2018 Annual Report, SC Cyber, cdn.ymaws.com/www.sccyber.org/resource/collection/D684A6A7-E0B8-45C2-939A-BBA5320F7DE6/20180805_-_SC_Cyber_Annual_Report_2017-2018_FINAL.pdf. Accessed 23 April 2019.

[87] "Cybersecurity Rules for Insurance Companies to Take Effect in South Carolina." Privacy & Information Security Law Blog, Hunton Andrews Kurth LLP, 2 Jan. 2019, www.huntonprivacyblog.com/2019/01/02/cybersecurity-rules-for-insurance-companies-to-take-effect-in-south-carolina/. Accessed 23 April 2019.

88 “Cybersecurity Rules for Insurance Companies to Take Effect in South Carolina.” Privacy & Information Security Law Blog, Hunton Andrews Kurth LLP, 2 Jan. 2019, www.huntonprivacyblog.com/2019/01/02/cybersecurity-rules-for-insurance-companies-to-take-effect-in-south-carolina/. Accessed 23 April 2019.

89 “Contact Us.” Department of Administration State of South Carolina, Department of Administration State of South Carolina, www.admin.sc.gov/technology/information-security/contact-us. Accessed 23 April 2019.

90 “U.S. Census Bureau QuickFacts: Spartanburg County, South Carolina.” Census Bureau QuickFacts, United States Census Bureau, 1 July 2018, www.census.gov/quickfacts/spartanburgcountysouthcarolina. Accessed 23 April 2019.

91 Montgomery, Bob. “After Cyberattack, Spartanburg Libraries Begin Checking out Books.” GoUpstate, GoUpstate, 1 Feb. 2018, www.goupstate.com/news/20180131/after-cyberattack-spartanburg-libraries-begin-checking-out-books. Accessed 23 April 2019.

92 Yee, Gregory. “Mount Pleasant Police Department Hit with Ransomware Cyberattack.” The Post and Courier, The Post and Courier, 27 Feb. 2018, www.postandcourier.com/news/mount-pleasant-police-department-hit-with-ransomware-cyberattack/article_40875fb4-c233-11e6-97cf-bf33fcb6f361.html. Accessed 23 April 2019.

93 “SC: Roper St. Francis Notifying Patients after Employees Fall for Phishing Attack.” DataBreaches.net, DataBreaches.net, www.databreaches.net/sc-roper-st-francis-notifying-patients-after-employees-fall-for-phishing-attack/. Accessed 23 April 2019.

94 Gilbert, Aleks. “Hacker Breaks into District 51 Computer.” Index-Journal, Index-Journal, 29 Jan. 2019, http://www.indexjournal.com/news/breaking/hacker-breaks-into-district-computer/article_364ac8e8-6535-54f0-9b2f-74b5270dc613.html. Accessed 23 April 2019.

95 “SC Cyber.” Fiscal Year 2018 Annual Report, SC Cyber, cdn.ymaws.com/www.sccyber.org/resource/collection/D684A6A7-E0B8-45C2-939A-BBA5320F7DE6/20180805_-_SC_Cyber_Annual_Report_2017-2018_FINAL.pdf. Accessed 23 April 2019.

96 Montgomery, Bob. “After Cyberattack, Spartanburg Libraries Begin Checking out Books.” GoUpstate, GoUpstate, 1 Feb. 2018, www.goupstate.com/news/20180131/after-cyberattack-spartanburg-libraries-begin-checking-out-books. Accessed 23 April 2019.

97 “S.C. National Guard Activates 1st Cyber Protection Unit.” Charleston Regional Business Journal, Charleston Regional Business Journal, 26 Oct. 2017, charlestonbusiness.com/news/defense/73210/. Accessed 23 April 2019.

98 “Computer Crime Center Staff.” South Carolina Law Enforcement Division, South Carolina Law Enforcement Division, www.sled.sc.gov/ComputerCrimesCenter.aspx?MenuID=ContactInformation. Accessed 23 April 2019.

99 “Homeland Security.” South Carolina Law Enforcement Division, South Carolina Law Enforcement Division, www.sled.sc.gov/HSOfficeHome.aspx?MenuID=HSOffice. Accessed 23 April 2019.

100 “SC Cyber.” Fiscal Year 2018 Annual Report, SC Cyber, cdn.ymaws.com/www.sccyber.org/resource/collection/D684A6A7-E0B8-45C2-939A-BBA5320F7DE6/20180805_-_SC_Cyber_Annual_Report_2017-2018_FINAL.pdf. Accessed 23 April 2019.

101 “Information Security.” Department of Administration State of South Carolina, Department of Administration State of South Carolina, admin.sc.gov/technology/information-security. Accessed 23 April 2019.

102 “About.” South Carolina Infragard, South Carolina Infragard, southcarolinainfragard.org/about. Accessed 23 April 2019.

103 “S.C. National Guard Activates 1st Cyber Protection Unit.” Charleston Regional Business Journal, Charleston Regional Business Journal, 26 Oct. 2017, charlestonbusiness.com/news/defense/73210/. Accessed 23 April 2019.

[104] "Field Offices." FBI, FBI, 3 May 2016, www.fbi.gov/contact-us/field-offices. Accessed 23 April 2019.

[105] "The Criminal Division." The United States Department of Justice, The United States Attorney's Office District of South Carolina , 30 May 2018, www.justice.gov/usao-sc/divisions/criminal-division. Accessed 23 April 2019.

[106] "South Carolina Electronic Crimes Task Force." LAW ENFORCEMENT CYBER CENTER, International Association of Chiefs of Police, www.iacpcybercenter.org/labs/south-carolina-electronic-crimes-task-force-2/. Accessed 23 April 2019.

[107] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[108] Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[109] "Clemson University Cybersecurity Center." Clemson University Cybersecurity Center, Clemson University, www.clemson.edu/centers-institutes/cybersecurity/index.html. Accessed 23 April 2019.

[110] "SC Cyber." Fiscal Year 2018 Annual Report, SC Cyber, cdn.ymaws.com/www.sccyber.org/resource/collection/D684A6A7-E0B8-45C2-939A-BBA5320F7DE6/20180805_-_SC_Cyber_Annual_Report_2017-2018_FINAL.pdf. Accessed 23 April 2019.

[111] "Center of Academic Excellence in Cyber Security." Department of Mathematics and Computer Science, South Carolina State University's Center of Excellence in Cybersecurity, mcs.scsu.edu/cybersecurity/. Accessed 23 April 2019.

[112] College, Trident Technical. "Cyber Center." Trident Technical College, Trident Technical College, www.tridenttech.edu/academics/divisions/bt/Center_for_Cybersecurity/Center_for_Cybersecurity.htm. Accessed 23 April 2019.

[113] Maucione, Scott. "Natl' Guard Cyber Units Protect Country's Interests, Still Face Training Issues." Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

[114] Maucione, Scott. "Natl' Guard Cyber Units Protect Country's Interests, Still Face Training Issues." Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

[115] Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 19. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 16 April 2019.

[116] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 23. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

[117] Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 19. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 16 April 2019.

[118] Federal Bureau of Investigation. "2017 Internet Crime Report." 22 June 2017, pp. 22. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 15 April 2019.

These figures do not necessarily provide a complete picture of Nevadans' economic losses because many cybercrime victims do not report their victimization to law enforcement. Source: Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New York Times, 5 Mar. 2018, http://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 16 April 2019.

119 “Nevada Office of Cyber Defense Coordination.” Nevada Office of Cyber Defense Coordination, Nevada Department of Public Safety, http://dps.nv.gov/uploadedFiles/dpsnvgov/content/divisions/OCDC/home/Nevada%20Office%20of%20Cyber%20Defense%20Coordination__Strategic%20Plan__2018%202020.pdf. Accessed 23 April 2019.

120 “Cybersecurity.” Nevada Governor’s Office of Science, Innovation & Technology, Nevada Governor’s Office of Science, Innovation Technology, osit.nv.gov/Cyber/Cyber/. Accessed 23 April 2019.

121 Bruzda, Natalie. “Cybersecurity Education Growing in Nevada as Threats Increase.” Las Vegas Review Journal , Las Vegas Review Journal , 20 May 2018, www.reviewjournal.com/news/education/cybersecurity-education-growing-in-nevada-as-threats-increase/. Accessed 6 Jun. 2019.

122 “SNCA Mission Statement.” Southern Nevada Cybersecurity Alliance, Southern Nevada Cybersecurity Alliance, snca.us/mission-statement/. Accessed 23 April 2019.

123 Hicks, Jordan. “Gov. Sisolak Encourages Young Women in School to Participate in Cyber Security Competition.” KRNV, Sinclair Broadcast Group, mynews4.com/news/local/gov-sisolak-encourages-young-women-in-school-to-participate-in-cyber-security-competition. Accessed 23 April 2019.

124 Conrad, Bob. “STATE: Fraudulent Unemployment Claims Targeted State Employees.” This Is Reno, This Is Reno, 19 Aug. 2016, thisisreno.com/2016/08/fraudulent-unemployment-claims-targeted-state-employees/. Accessed 23 April 2019.

125 “Cyber-Attack on Nevada Medical Marijuana Program Compromises Employee Info.” KRNV, Fox11, 28 Dec. 2016, mynews4.com/news/local/cyber-attack-leads-to-leak-of-nevada-medical-marijuana-employee-owner-info. Accessed 23 April 2019.

126 Ragan, Steve. “Hard Rock Las Vegas Suffers a Second Data Breach.” CSO Online, CSO, 28 June 2016, www.csoonline.com/article/3089449/hard-rock-las-vegas-suffers-a-second-data-breach.html. Accessed 23 April 2019.

127 “Las Vegas Sands’ Network Hit by Destructive Malware in Feb: Bloomberg.” Reuters, Thomson Reuters, 12 Dec. 2014, www.reuters.com/article/us-lasvegassands-cybersecurity/las-vegas-sands-network-hit-by-destructive-malware-in-feb-bloomberg-idUSKBN0JQ04520141212. Accessed 23 April 2019.

128 Murphy, Vanessa, and Bill Roe. “I-Team: Cyber Attacks Have Cost Las Vegas Businesses Millions.” LASVEGASNOW, LASVEGASNOW, 23 Nov. 2016, www.lasvegasnow.com/news/i-team-cyber-attacks-have-cost-las-vegas-businesses-millions/611564579. Accessed 23 April 2019.

129 “Cybersecurity Center.” Cybersecurity Center, University of Nevada, Reno, www.unr.edu/cybersecurity. Accessed 23 April 2019.

130 “Nevada Office of Cyber Defense Coordination.” Nevada Office of Cyber Defense Coordination, Nevada Department of Public Safety, http://dps.nv.gov/uploadedFiles/dpsnvgov/content/divisions/OCDC/home/Nevada%20Office%20of%20Cyber%20Defense%20Coordination__Strategic%20Plan__2018%202020.pdf. Accessed 23 April 2019.

131 “SNCA Mission Statement.” Southern Nevada Cybersecurity Alliance, Southern Nevada Cybersecurity Alliance, snca.us/mission-statement/. Accessed 23 April 2019.

132 “Nevada Office of Cyber Defense Coordination.” Nevada Office of Cyber Defense Coordination, Nevada Department of Public Safety, http://dps.nv.gov/uploadedFiles/dpsnvgov/content/divisions/OCDC/home/Nevada%20Office%20of%20Cyber%20Defense%20Coordination__Strategic%20Plan__2018%202020.pdf. Accessed 23 April 2019.

133 “About the Nevada Division of Emergency Management.” About DEM, Department of Public Safety, dem.nv.gov/About/Overview/. Accessed 23 April 2019.

134 “About Us.” Office of Nevada Consumer Affairs, Department of Business and Industry, consumeraffairs.nv.gov/About/About__Us/. Accessed 23 April 2019.

135 “Technological Crime Board.” Tech Crime Board, Nevada Attorney General, ag.nv.gov/About/Administration/Tech__Crime__Board/. Accessed 23 April 2019.

[136] “Criminal Division.” The United States Department of Justice, The United States Attorney’s Office District of Nevada, 16 Apr. 2019, www.justice.gov/usao-nv/criminal-division. Accessed 23 April 2019.

[137] “Field Offices.” FBI, FBI, 3 May 2016, www.fbi.gov/contact-us/field-offices. Accessed 23 April 2019.

[138] “Homeland Security Investigation Principal Field Offices.” ICE, United States Department of Homeland Security, www.ice.gov/contact/hsi. Accessed 23 April 2019.

[139] “Find a Field Office.” Field Offices, United States Secret Service, www.secretservice.gov/contact/field-offices/. Accessed 23 April 2019.

[140] Eoyang, Mieke, et al. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[141] Eoyang, Mieke, et al. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” Third Way, Third Way, 29 Oct. 2018, https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 15 April 2019.

[142] “Cybersecurity Center.” Cybersecurity Center, University of Nevada, Reno, www.unr.edu/cybersecurity. Accessed 23 April 2019.

[143] “Cybersecurity Center.” Cybersecurity Center, University of Nevada, Las Vegas, www.unlv.edu/program/cybersecurity. Accessed 23 April 2019.

[144] Maucione, Scott. “Natl’ Guard Cyber Units Protect Country’s Interests, Still Face Training Issues.” Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.

[145] Maucione, Scott. “Natl’ Guard Cyber Units Protect Country’s Interests, Still Face Training Issues.” Federal News Network, Federal News Network, 18 Jan. 2019, federalnewsnetwork.com/defense-main/2019/01/national-guard-cyber-units-protect-countrys-interests-still-face-training-issues/. Accessed 22 April 2019.