A REPORT BY THE

SPECIAL SENATE COMMITTEE ON CYBER SECURITY READINESS

MASSACHUSETTS
SENATE
08.15.18

Committee Members

Michael O. Moore
Chair

Second Worcester District
Consisting of the Towns of Auburn, Grafton, Leicester, Millbury, Northbridge, precincts 2 and 4, Shrewsbury and Upton and the City of Worcester, wards 5 to 7, inclusive, and ward 8, precincts 1 and 5 in the County of Worcester.

Cynthia S. Creem
Vice Chair

First Middlesex and Norfolk District
Consisting of the City of Newton in the County of Middlesex; and the Towns of Brookline and Wellesley, precincts A, C to E, inclusive, and H in the County of Norfolk.

Michael D. Brady
Member

Second Plymouth and Bristol District
Consisting of the City of Brockton and the Towns of East Bridgewater, precincts 1 to 3, inclusive, Halifax, Hanover, Hanson, Plympton and Whitman, all in the County of Plymouth; and the town of Easton, precincts 1 and 2, in the County of Bristol.

Eric P. Lesser
Member

First Hampden and Hampshire District
Consisting of the Cities of Chicopee, ward 1, precincts A and B, ward 5, precincts A and B, ward 6, precincts A and B, ward 8, precinct B and ward 9, precinct B and Springfield, ward 2, precinct G, ward 4, precinct F, ward 5, precincts D, F, G and H, ward 6, precincts B, D and H, ward 7 and ward 8, precinct A and the Towns of East Longmeadow, Hampden, Longmeadow, Ludlow and Wilbraham in the County of Hampden; and the Towns of Belchertown and Granby in the County of Hampshire.

Ryan C. Fattman
Member

Worcester and Norfolk District
Consisting of the Towns of Blackstone, Douglas, Dudley, Hopedale, Mendon, Milford, Millville, Northbridge, precincts 1 and 3, Oxford, Southbridge, Sutton, Uxbridge and Webster in the County of Worcester; and the Town of Bellingham in the County of Norfolk.

Table of Contents

I. COMMITTEE FACTS AND HISTORY

Executive Summary

In an effort to combat the heightened cyber risk of today's society, the Senate of the Commonwealth of Massachusetts formed the Special Senate Committee on Cyber Security Readiness ("the Committee") on May 3, 2017, via Senate Order No. 2060. The Committee is composed of five senators, four appointed by the President of the Senate and one appointed by the Minority Leader of the Senate. These members are Sen. Michael O. Moore, Chair, D – 2nd Worcester; Sen. Cynthia Stone Creem, Vice Chair, D – 1st Middlesex & Norfolk; Sen. Michael D. Brady, D – 2nd Plymouth & Bristol; Sen. Eric P. Lesser, D – 1st Hampden & Hampshire; and Sen. Ryan C. Fattman, R – Worcester & Norfolk. The Committee was charged to "review and make recommendations for the state to improve its cyber security readiness, enhance technological responses to homeland security and public safety threats, and further protect financial, medical and other sensitive information."

The Committee has found that the state is in a particularly vulnerable position when it comes to preparedness for cyberattacks. There is a need for more strictly regulated and enforced cybersecurity measures in both the public and private sectors, which leaves the private data of Massachusetts citizens open to manipulation and theft, actions which can ruin companies' reputations and destroy public trust in government bodies. In addition to the danger posed to private datasets, the lack of strong cybersecurity measures within the state have the potential to disrupt critical elements of infrastructure. A disruption in this critical societal function poses a physical threat to the wellbeing of Massachusetts citizens.

With this in mind, the Committee is recommending the creation of a standing joint committee in the legislature to address bills related to the topic of cybersecurity. They also

recommend the creation of a Cybersecurity Control and Review Board ("CCRB"), a five-person oversight committee that would be made up of private sector and cybersecurity representatives, and tasked with improving cybersecurity across businesses in the Commonwealth. The Committee's findings and recommendations for further action on the issue of cybersecurity are discussed in detail within this report.

Significance

As technology progresses, more and more of modern life takes place on computers, smartphones, and other interconnected devices. The influx of these devices has numerous benefits for society, but with these benefits come great risk to consumer data, privacy, safety, and security. Cyber criminals tend to target technological, financial, health care, and educational institutions due to the large amounts of private data these corporations gather. For example, in 2013, Yahoo suffered a major data breach on their servers, losing personal information about all 3 billion users to hackers. In 2014, Yahoo suffered from a similar attack, this time losing the personal information of 32 million accounts. In 2017, Yahoo was again compromised, resulting in the loss of private information and login credentials of over 200 million users. These hacks cost the company over 350 million dollars, as well as destroyed their reputation as a safe place for correspondence. Tax giant Equifax announced on September 7, 2017 that they had suffered a major breach of their information databases in May of 2017. The hack resulted in the loss of personal information of over 145 million users, nearly half of the United States population, including credit card numbers, addresses, and social security information. This attack cost Equifax over $600 million in revenue and reparations, as well as destroyed the reputation of the company.

This type of cybercrime, known as a data breach, is far from the only type of cybercrime in existence. Many cyberattacks focus on compromising the hardware a company or community uses to operate—utilities, voting machines, transportation systems, and servers. This type of attack can be targeted against private businesses, such as the attack that occurred against American code conglomerate GitHub on February 28, 2018, when GitHub suffered the largest distributed denial of service (DDoS) attack in history. Bots overwhelmed the company's servers with thousands of fake transaction requests, causing the site to shut down for eight minutes. This period of time cost the website and the developers that make use of its services millions of dollars in lost revenue.

Another major type of cybercrime is known as ransomware, a malicious virus that locks down files within a computer until a ransom is paid. The largest ransomware attack in history occurred in May of 2017, when the WannaCry Ransomware attacked hundreds of thousands of computers worldwide, including private-use laptops, company computers, and state-connected devices. This malware quickly spread through connected systems via vulnerabilities in Windows software. It stole user data and encrypted the computer's files, forcing users to pay a ransom if they wanted to access stored information. The quick spread of this ransomware cost private citizens and companies over eight billion dollars, and resulted in the loss of vital documents across the globe. The total projected cost of these attacks to the global economy is over $53 billion.

Ransomware can have a major impact on the operations of governments and businesses. On March 22, 2018, Atlanta was hit with the largest ransomware attack on an American city. Hackers locked down the city's connected infrastructure for five days, demanding over $50,000 worth of Bitcoins to return the files. During this time city employees had no access to work

computers, Atlanta residents could not pay utilities bills or traffic tickets, and years' worth of critical police evidence tapes were destroyed. The damages resulting from the attack cost the city of Atlanta over $2.7 million, and destroyed public confidence in the Atlanta government's ability to uphold their digital infrastructure.

Current Massachusetts Cybersecurity Measures

The examples of major cyberattacks discussed in the "Significance" section of the report are simply a smattering of the cybercrimes that have occurred against governments, businesses, and private citizens in recent years. Massachusetts is in an extremely vulnerable position when it comes to the protection of its cyber systems, as evidenced by recent breaches in the towns of Holyoke, Leominster, and Brookline.

Massachusetts is currently using a strategic plan to combat cybercrime developed in 2007. The 2007 cybercrime strategic plan outlines a clear mission to respond to cybercrime, focusing on assisting law enforcement to investigate and prosecute crimes committed on or using a computer after they have occurred. The plan also provides goals and objectives for gauging progress in order to deliver the highest level of public safety to the citizens of Massachusetts. However, the plan was not intended to be a comprehensive blueprint for the state, and does not address measures that businesses, private citizens, federal partners, municipalities, or other state government agencies could put into place in order to deter cyberattacks before they occur, and is neither regulated nor enforced. In addition, the strategic plan focuses primarily on assisting local law enforcement agencies and was not intended to address cybercrime and cybersecurity at the state level.

In addition to the general strategic plan, specific anti-cyberterrorism measures were developed by the state Homeland Security Division in 2014. These measures include promoting

public-private cooperation, strengthening Massachusetts' critical infrastructure, and implementing staff training. However, with no way to ensure that these measures are occurring, and no way to enforce their implementation, these measures are not being used in the Commonwealth.

The Massachusetts Executive Office of Technology Services and Security also developed a set of strategic priorities for cybersecurity in the Executive Department in 2016. This set consists of six streams of further work into cybersecurity matters: risk and compliance assessment, identity and access management, network security engineering, vulnerability management, incident response, and data specific security. The EOTSS has also created specific suggested actions for each of these topics, based off the federal NIST Cybersecurity Framework (see "Regulations Across the United States"). Despite the commendable goals and efforts of the EOTSS, they do not have the ability to ensure that all departments under their jurisdiction are following through with their proposed cybersecurity regulations.

One of the greatest problems exacerbating the issue under discussion is that the government of Massachusetts has yet to determine a concrete definition for what types of actions fall under the realm of cybersecurity, greatly widening the scope of the problem and causing confusion for anyone attempting to work on a solution. Cybersecurity can refer to the security of the government itself, or it can refer to the security of businesses in the private sector. It is used in reference to both protection of data, such as names, addresses, and social security numbers, as well as the protection of critical infrastructure ("CI"), such as utilities, transportation, and voting machines. Cybersecurity at the government level can also be used when discussing the lack of technically qualified employees in state and local governments, as well as the necessity of strong computer science education in college and K-12 schools. These topics all fall under the umbrella

of “cybersecurity,” yet cover a wide range of subjects, each necessitating experts with very different interests and skill sets.

When it comes to the private sector, businesses are subject to even less regulation, as the impetus to monitor and enforce quality cybersecurity measures as regulated by 201 CMR 17 are left to the jurisdiction of each company. Without a way to ensure that private companies are doing everything in their power to protect the confidentiality and integrity of their users’ data, citizens across the Commonwealth are put at risk. Another factor that complicates cybersecurity matters is that in many cases, especially surrounding CI, it is unclear where public jurisdiction ends and where private jurisdiction over cybersecurity matters begins.

As mentioned, the CI in Massachusetts is especially at risk. This category includes electric, gas, and water utilities, voting systems, and transportation and banking infrastructure, and incorporates both public and private organizations. Many cities and towns are running electric, gas, and water utilities on outdated, vulnerable technology especially prone to even basic attacks by semi-committed bad actors. In addition, private contractors working in these fields are allowed to self-certify, making it difficult to gauge how prepared they are for a cyberattack, as well as difficult to make any improvements to existing cybersecurity measures.

The Department of Public Utilities (DPU) regulates water, gas, and electric utilities throughout the commonwealth. Their cybersecurity plan relies on self-certifying and self-reporting, which may leave the citizens of Massachusetts vulnerable to both data loss and utilities disruptions, and has the potential to cause the state’s economy to lose millions of dollars in lost revenue. While the DPU has cybersecurity procedures in place, the state has paid little attention to its regulation and enforcement. Transmission facilities, responsible for delivering vital electricity to millions of Massachusetts citizens, are an especially vulnerable element of

Massachusetts' infrastructure. The standards currently used to regulate transmission sites come from NERC CIP (see "Regulations Across the United States"), and only covers facilities that transmit over 100kV. For comparison, the substations that provide for the Boston area typically transmit around 34kV, not nearly enough to trigger NERC CIP attention. By not requiring NERC CIP regulations, transmission sites are exempt from cybersecurity regulation, leaving the cities and towns they service vulnerable to a service disruption. This issue is compounded due to the fact that the majority of transmission sites within municipalities are connected via a transmission line. A hacker with malicious intent could break into a single transformer station with relative ease, and take over the utilities for an entire city or town. Currently, Massachusetts has no way to regulate and ensure transmission stations are prepared for this type of attack.

Regulations Across the United States

Massachusetts, typically a trailblazer in technological policy, is currently lacking in its cybersecurity plans and tactics. Several other states have successfully implemented cybersecurity plans for both their public departments and private companies conducting business within their state.

California has emerged as a leader in cybersecurity policy amongst states. Their cybersecurity programs focus on updating technology and implementing staff training in order to ensure the state is prepared for cyber threats. They are focusing the majority of their efforts into preparing and training their IT workforce to provide for cybersecurity and deal with cybercrimes.

Iowa is another major player in the cybersecurity arena. They have focused their energy into two main areas: protecting CI and protecting data of state citizens. They have implemented staff training across government sites, collaborated with the private sector, and established and

implemented emergency response plans for ensuring government and businesses still function during and after a breach.

Virginia's cybersecurity plan is focused on concentrating the various cyber-vulnerable elements of their state government into a single, more easily defendable location. This includes developing a single user identification system for their state, updating their technology, and implementing consistent monitoring and testing of their cybersecurity systems.

In addition to regulation done by the states, the federal government has provided a list of guidelines to help states, individuals, and private companies assess and improve their cybersecurity measures. The largest and most comprehensive of these guidelines is the National Institute of Standards and Technology (NIST) cybersecurity framework. Updated in 2018 and used by 20 states and 30% of major American organizations, the NIST framework is a comprehensive set of guidelines that assist companies and governments in assessing the status of their cybersecurity, determining reasonable goals for cybersecurity improvements, and providing concrete steps and resources in order to reach those goals. The Federal Energy Regulation Commission (FERC) is responsible for regulating the cybersecurity preparedness of utilities in the United States. In 2006, FERC certified the North American Electric Reliability Commission (NERC) to create the regulations for utility departments. NERC regulations, while comprehensive, are neither required nor enforced. In addition, as mentioned in the "Significance" section of this report, they do not apply to every utility used by in the Commonwealth, only those that generate a certain amount of power or supply service to a certain number of people.

II. MEETING HISTORY

Meeting #1 – June 6, 2017

The Committee first met to review the Committee's purpose and to identify public-sector areas of concern. These areas included evaluating existing systems and protocols, protecting data from criminals, understanding motivations for cybercrime, and determining funding needs. The Committee also recognized the need to support the private sector in cybersecurity matters.

The Committee identified several potential site-visit hosts, including both public and private sector organizations. These included the Massachusetts Executive Office of Technology Services and Security (EOTSS), National White Collar Crime Center (NW3C), and Pricewaterhouse Coopers (PwC) Cybersecurity Division.

Meeting #2 – October 3, 2017

The Committee spent the first hour meeting with Mr. Christopher W. Kelly, Director of the Massachusetts Attorney General's Digital Evidence Laboratory. Mr. Kelly discussed several challenges facing both public and private entities concerned with security and provided several ideas for future legislation. His expertise comes from an ex post perspective—his office evaluates computer systems, mobile devices, social media, and open data pertinent to ongoing investigations.

Mr. Kelly identified inadequate resources as the single most critical challenge his office faces in their daily operations. The hardware and software needed to run digital forensic investigations are expensive, and qualified individuals can easily find better pay from the private sector. Training for new staff is also prohibitively expensive given his office's current budget.

Another main concern of Mr. Kelly's is the scope of the problem. "Cyber" is a nebulous concept that needs to be clearly defined to set the bounds of any issues the Committee will

address. Mr. Kelly identified two main areas that fall under the "cyber" concept and are in dire need of protection: critical infrastructure (water and electric utilities, 911 response, etc.) and data (personally identifiable information ("PII"), social security numbers, etc.).

Mr. Kelly proposed several legislative solutions to begin addressing these concerns. First, he noted that there is presently no monitoring of companies' use of legally mandated data encryption. Firms may be fined after a breach, but at that point the harm has been done. Next, he noted that 3rd party vendors charge state agencies up to $2,000 to decrypt a device—a prohibitively high cost that could benefit from regulatory measures. He also recommended revising M.G.L. ch. 266, S 120 for clarity; perhaps modeling changes off California's aggressive statutory regime (see "Regulations Across the United States").

The Committee next heard from Mr. Dennis McDermitt, Chief Security & Technology Officer of the Executive Office of Technology Services & Security. Mr. McDermitt has spent his 20-year professional career leading cybersecurity organizations in both public and private sectors, working with weapons systems, financial systems, and both critical infrastructure and sensitive data. Mr. McDermitt described the dynamic nature of cybersecurity, delineated between compliance and readiness, and provided several ideas for future legislation.

Mr. McDermitt identified three dimensions of cybersecurity: confidentiality, integrity, and availability. Integrity here refers to the need to maintain public trust in critical institutions such as healthcare and financial service providers. Availability concerns the assets that are susceptible to hacks, including cars, building heating and cooling systems, and utilities, and the unsuspecting assets that may be used to initiate an attack. For example, Mr. McDermitt discussed a recent Denial-of-Service attack that used internet-connected thermostats to flood a U.S.-based internet service provider with superfluous requests for information from servers, blocking

legitimate server requests and shutting down the service provider for several minutes. He next identified the main targets of cybercriminals: data, for use in identity theft; cybercrime, or multidimensional use of data for nefarious ends; and critical infrastructure, including utilities, internet-connected services, and election systems.

Mr. McDermitt also made a number of recommendations for actions that can reduce cybersecurity risk. First, he noted the importance of critical infrastructure as a high-priority item, given the grave real-world consequences of those systems becoming unavailable. Along those lines, he discussed the benefits of regular testing of utilities' cyber-infrastructure. Next, he recommended implementing the white-hat hacker approach to cybersecurity, which involves a friendly actor attempting to breach an organization's digital assets and providing a report that allows for the organization to patch deficiencies, a process also known as "red teaming." He also described the importance of election infrastructure, but noted that such infrastructure falls within the purview of the Secretary of the Commonwealth.

The second hour of the meeting included the Committee discussing the information provided by Mr. Kelly and Mr. McDermitt.

Meeting #3 – October 17, 2017

The Committee spent the first hour meeting with Mr. Brandon C. Brin, IT Director for Legislative Information Services ("LIS"). Through his work with LIS, Mr. Brin has gained invaluable expertise in the data security field, and was invited to speak on the topic at the National Conference of State Legislatures ("NCSL") 2017 Legislative Summit. During the course of the meeting, Mr. Brin provided the Committee with multiple suggested areas of focus. His proposal identifies a wide array of areas that deserve the Committee's attention.

The first area identified was consumer awareness surrounding cybersecurity concerns and public disclosure of data and system breaches. Mr. Brin recommended that the Committee should pursue a policy of increasing public awareness regarding identity theft, digital extortion, and online fraud. An important part of this policy is developing the requirements for private-sector data breach reporting. In order to preserve full transparency and preserve the public trust, breaches must be reported to law enforcement, regulatory agencies, and ultimately consumers. Analyzing the response to prior cybersecurity breaches may also yield valuable insight into how such policies should be structured.

Cybersecurity training and cybersecurity education in schools was the next area of focus Mr. Brin discussed. He suggested that comprehensive cybersecurity education should begin in elementary and secondary schools, and that the public school curriculum should incorporate cybersecurity-related topics into any STEM-focused curriculum initiatives currently under implementation. In addition to education, Mr. Brin also went over recommendations surrounding public and private sector employees and training regimens. Guidelines establishing training for state and municipal government employees, especially those handling financial transactions or sensitive personal information, should be developed and implemented. In addition, private sector employee training should also be addressed by the Committee. While 201 CMR 17.00 mandates training for private-sector entities handling personal information, there is currently no method of enforcing the regulation's requirements, a grave vulnerability that should be addressed in future legislative discourse. Mr. Brin suggested that the regulations in 201 CMR 17.00 should also be expanded upon to respond to industry-specific concerns and to increase the visibility of cybersecurity awareness.

The next area addressed was private and public sector engagement, including engagement between industry and government as well as engagement between academia and government. Mr. Brin recommended a highly centralized cybersecurity coordination effort, where a single entity would be charged with coordinating information sharing across state and municipal agencies, assisting with private-sector engagement, and identifying best practices to be widely implemented. This type of partnership is especially critical when it comes to private infrastructure providers, who need to have a close working relationship with government entities to ensure they are prepared to protect these high-value targets. These infrastructure providers should similarly have an emergency response plan. This plan should be developed in coordination with an array of stakeholders to prepare for "worst case scenarios" and subsequently tested and updated to ensure effectiveness. The government should also partner with academics focusing on cybersecurity research within Massachusetts, supporting their work by creating a safe atmosphere with which to come forward about vulnerabilities in existing systems. Researchers should be empowered to notify government agencies and individuals of these flaws without fear of legal repercussions.

In addition to protecting personal data and developing cybersecurity contingency plans, Mr. Brin stressed the importance of empowering law enforcement, investigators, and prosecutors to deal with the growing influx of cybercrime, defined as crimes which leave a digital evidence trail or take place primarily over an internet-connected device. Law enforcement agencies may need unique training and additional resources to combat cybercrime. When it comes to the court system the decentralized nature of internet-based crimes makes prosecution difficult, a hurdle which may be addressed via legislation that is responsive to these modern crimes.

The final topic discussed focused on coordination within the state government and within critical government agencies themselves. Interagency engagement, baseline security standards, and training are all necessary to ensure institutional preparedness. Government agencies, much like private sector entities, need comprehensive emergency response plans with separate plans to deal with the various types of cybersecurity-related threats. These plans uniquely require interagency and intra-agency coordination, short and long term continuity plans to keep services available during an emergency, and backup communication plans that do not rely on internet and cellular phone networks.

Meeting #4 – November 8, 2017

The Committee discussed the scope of the Committee's subject matter, distilling which issues are to be addressed by the state and which issues are already covered by federal statutes and regulations; potential regulatory requirements in the prevention, detection, and response phases of a cybersecurity plan; and which existing, or perhaps new, state agency or agencies will have jurisdiction over public sector cybersecurity.

First, the Committee identified three principal areas of concern: State and Municipal Critical Infrastructure, Non-State Critical Infrastructure, and Information Privacy. Decisions on what to address in future legislation will require coordination with federal statutes and regulations to prevent unwanted redundancy and fill any gaps.

Next, the Committee identified potential regulatory requirements relevant to cyberattacks, including mandatory training for state employees involved in infrastructure protection. Another regulatory approach involves mandating a testing protocol where a friendly actor attempts to hack into certain computer systems to test their cybersecurity protocol efficacy and identify gaps that need to be addressed, a process known as "red teaming." Regulatory requirements can also

be implemented to mandate that organizations implement detection procedures and develop a response plan that guides the organization's post-breach response.

Finally, the Committee considered how to delegate responsibility for implementing a cybersecurity regulatory regime. Options included: creating a new agency, empowering an existing agency with additional authority over cybersecurity issues, and empowering an existing agency with additional authority over cybersecurity issues by decentralizing the process via the assigning of authority to multiple relevant agencies. This last approach facilitates industry-focused specification by allowing for varying requirements in order to meet the needs of a given sector. This recognizes that different industries use different types of data and have different types of infrastructure such that the regulators that monitor a given industry may need unique skills that are not relevant to other industries.

III. RECOMMENDATIONS AND NEXT STEPS

The Special Senate Committee on Cyber Security Readiness offers the following recommendations:

Standing Joint Committee

The Legislature should establish a new Standing Joint Committee on Cybersecurity to review and propose legislation. An increasing amount of legislation will concern infrastructure protection and data privacy, and it is essential that a committee with a permanent charge is established to advise the Legislature on these matters.

Cybersecurity Control and Review Board

The Legislature should establish a Cybersecurity Control and Review Board ("CCRB") in order to regulate and oversee cybersecurity matters in the commonwealth. The CCRB would be a 5-member advisory board comprised of individuals knowledgeable about sector-specific cybersecurity matters. The proposed list of sectors include: business, financial, health, utilities, and a general cybersecurity specialist. The CCRB will report to the new Secretariat and will provide the Legislature with recommendations for legislation, capital allocations, and infrastructure needs related to cybersecurity issues across the Commonwealth.

The CCRB's roles and responsibilities are as follows:

1. The CCRB will conduct a study of Massachusetts' current cybersecurity measures.
    i. They will conduct the study for the Massachusetts government.
    ii. They will provide resources and assistance to any private companies seeking to assess the strength of their cybersecurity preparedness.
2. The CCRB will create, adopt, and review regulations for:
    i. Data protection standards;
    ii. A recommended standard cybersecurity accreditation classification;
    iii. A model protocol for responding to data breaches;
    iv. Cybersecurity curriculum initiatives for elementary, middle, and high schools, to be reported to the Massachusetts Department of Elementary and Secondary Education (DESE);
    v. Minimum training standards for public and private employees; and
    vi. Recommended state standards for future software acquisitions by public agencies.
3. The CCRB will enforce the above determined guidelines in Massachusetts government offices and state-accredited corporations.

4. The CCRB will continuously test, monitor, and improve the strength of Massachusetts' cybersecurity in both state and municipal government offices and businesses approved by the state as cyber secure.
5. The CCRB will develop and implement mandatory self-auditing standards for private corporations and public agencies entrusted with protecting data and critical infrastructure.

Appendix A – Senate Order No.2060

Ordered, that there shall be a special committee on the part of the Senate on cyber security readiness. The committee shall consist of 5 members of the Senate, 4 of whom shall be appointed by the President of the Senate and 1 of whom shall be appointed by the Minority Leader of the Senate. The committee shall review and make recommendations for the state to improve its cyber security readiness, enhance technological responses to homeland security and public safety threats, and further protect financial, medical and other sensitive information. The committee shall file its report, with any recommendations for legislation, with the clerk of the senate by March 30, 2018.

Appendix B – Meeting #1 Agenda

Agenda

1. Welcome
2. Purpose of the Committee
    a. High-profile cybercrimes (Sony, DNC Hack, Target)
    b. Increased vulnerability
3. Areas of Interest – Public Sector Concerns
    a. Evaluation of existing cybersecurity systems, protocols
        i. Interagency collaboration/consistency (state-state, state-federal)

b. Data protection from criminal use – data is valuable in and of itself, and as a means to further fraud
    i. Internal threats
        1. Both active internal breaches and "risk-conscious" workforce
            a. Government owned devices vs. personal devices
            b. Social media as a possible entry point
        2. Leveled security privileges, matching requirements
    ii. External threats
        1. Targeted attacks vs. large scale
        2. Attacks on outside industries (financial, healthcare, energy) could leave us vulnerable in other areas
        3. Methods are quickly increasing in sophistication
    iii. Third-party (i.e. state contractors)
c. Cybercrime as a service/cyber-terrorism attacks—aim is disruption
    i. Protections vs. responses
    ii. As potential for cybercrimes increases, there will be individuals who offer the technical cybercrime expertise to others for a price
        1. Targets could be government, businesses, individual citizens
d. Budgetary needs—short and long term
e. Non-Public Sector Cybersecurity Concerns
    i. Private consumer data
    ii. Broader internet privacy issues

4. Additional Areas of Interest—Any suggestions?
5. Potential Meetings or Site-Visits
    a. MassIT (Office of Information Technology)
        i. Executive Director Mark E. Nunnelly
        ii. Took over March 2016, likely has begun or completed much of the analysis about existing cybersecurity that we may want to see
    b. National White Collar Crime Center (NW3C)
        i. Congressionally funded non-profit that trains state/local law
        ii. Tyler Wotring, Cyber Crimes Section Supervisor has offered resources

c. British Consulate
    i. A former officer from GCHQ (Government Communications Headquarters), the primary intelligence gathering agency in Britain, now teaches at the Belfer Center (Harvard, international security and diplomacy, as well as science and technology)
    ii. Offering their relationships with several British-based companies, some with locations in Boston
d. Northeastern University Cybersecurity and Privacy Institute
    i. Set to open this summer
    ii. Will be led by former Google Director of Engineering (previously Microsoft)
e. Private Industry—Major concern for many businesses/trade groups
    i. PricewaterhouseCoopers (PwC)
        1. Cybersecurity division that has done work with multiple public agencies inside and outside of Massachusetts
        2. Game of Threats—workshop simulation to teach about vulnerabilities and test best practices (MassDOT)
    ii. Associated Industries of Massachusetts (AIM)
        1. Interested in offering assistance on consumer data side
    iii. Verizon—publishes a yearly report on data breaches

6. Legislation
    a. Handful of cybersecurity specific bills
    b. Many bills that deal with internet privacy and other issues that touch upon cybersecurity issues

Appendix C – Meeting #2 Agenda and Notes

Agenda

1. Welcome
2. Guest Presentations
    a. 12:00pm – 12:30pm: Christopher W. Kelly, Director, Digital Evidence Laboratory, Commonwealth of Massachusetts, Office of the Attorney General.

b. 12:30pm – 1:00pm: Dennis McDermitt, Chief Security & Technology Officer, Executive Office of Technology Services and Security (EOTSS).

3. Discussion and Next Steps
    a. 1:00pm – 2:00pm: Committee discussion regarding future speakers and next steps

Presenter Biographies

Christopher W. Kelly, *Director, Digital Evidence Laboratory*
Office of the Massachusetts Attorney General

Chris Kelly is the Director of the Digital Evidence Laboratory for the Massachusetts Attorney General's Office. In this role, Chris supervises a team of analysts conducting digital forensic examinations of computers, mobile devices, and other technical evidence in the course of criminal investigations. Prior to his appointment to this position, Chris served as Managing Attorney of the Cyber Crime Division for the Massachusetts Attorney General's Office. In that position, Chris not only prosecuted cyber offenses, but also worked with members of the Cyber Crime Division to design and implement priority projects and trainings as set forth in the Massachusetts Strategic Plan for Cyber Crime. Before joining the Attorney General's Office, Chris worked for the Suffolk County District Attorney's Office, where he built and ran the current Computer Forensic Laboratory. During his tenure in Suffolk, Chris prosecuted cybercrime cases and worked actively on digital aspects of all types of criminal investigations. Chris holds several digital forensic certifications including the GCRA, DFCP, CCE, CCME, EnCE, and CCLO/CCPA. He is a regular speaker on topics related to digital forensics and cybercrime investigations. Additionally, Chris serves as an instructor and performs curriculum development for the United States Secret Service's National Computer Forensic Institute in Hoover, Alabama. He is an adjunct professor of digital forensics at Bunker Hill Community College in Boston. Chris serves as a leader or active member of several professional associations

including the High Technology Crime Investigation Association, International Association of Chiefs of Police Cyber Crime and Digital Evidence Committee, High Tech Crime Consortium, and American Academy of Forensic Science Digital and Multimedia Sciences Section. Chris is a member of the Accreditation Task Group for the National institute of Standards in Technology's Digital Evidence subcommittee of the Organization of Scientific Area Committees for Forensic Science. He also sits on the editorial board for the Journal Digital Investigation, and reviews articles for the Journal of Digital Forensics, Security and Law. Chris earned bachelor's degrees in psychology and political science from Boston University, and his law degree from Suffolk University Law School.

Dennis McDermitt, *Chief Security & Technology Officer*
Executive Office of Technology Services and Security (EOTSS)

Dennis McDermitt is the Chief Information Security Officer and Chief Technology Officer of the Executive Office of Technology Services and Security in the Commonwealth of Massachusetts. He has more than twenty years of experience leading complex cybersecurity, software, and technology services organizations in both the public and private sectors. Dennis has led more than fifty classified programs and implemented a variety of highly secure systems related to nuclear weapons, finance, and other national security concerns. He also has extensive experience implementing secure public cloud solutions for critical infrastructure and sensitive data. Dennis earned a Master of Science degree in Computer Science from Johns Hopkins University and has completed advanced post-graduate work in business and finance at Imperial College London and the MIT Sloan School of Management.

Presentation Notes

Chris Kelly, *Director, Digital Evidence Laboratory*
Massachusetts Attorney General's Office

- Focused on digital forensics within criminal AG's investigations and sometimes also work with police departments and district attorney's offices
    - In an investigation, will look at computer systems, mobile devices, social media, open data
    - Typically operate under a search warrant
        - Have admin subpoena authority under a state enabling statute of federal protection
            - AAsG and ADAs can issue a state administrative subpoena for basic subscriber info only under state statute which acts in conjunction with federal ECPA and SCA
        - Doesn't have administrative warrant authority
    - Can't speak from IT/prevention side, his lab doesn't work on prevention
- Challenges
- Need to define the word "cyber." Nebulous; scope of problem is unclear
    - Not enough federal data
        - Need and current push to accurately define scope of "cybercrime" so that reporting of incidents is done at the federal level. Must be made part of annual crime reporting stats so that appropriate funding and resources start to funnel to state and local jurisdictions
    - Don't have enough resources
        - People—trained/qualified personnel can find more lucrative options outside of state government
        - Hardware and software is very expensive
            - E.g. majority of cases involve mobile devices. Need to use third party vendor to decrypt mobile devices and this can cost $2000 per device. Vendor also will not sell software.

            - E.g. have three vans, which are $13000 each +$4000/year to maintain—have 3, need more
        - Cost of specialized training is prohibitive
            - E.g. special training is $4000 x 8 employees = $32000, which is more than their annual budget
- Traditional cyber expenses within "cyber" category
    - Ransomware
    - Data hacking
    - Threats/extortion/online posting (e.g. revenge porn)
    - Doxing—searching for and publishing private or identifying information about a particular individual on the Internet, usually with malicious intent
- Cyber security model: prevention, detection, response
- First steps: First focus has to be infrastructure/data protection (data = social security numbers, personal info; critical infrastructure = it infrastructure, electric grid, water utilities, 911 response, etc.)
    - Address with hardware/software ; protect the network
    - Work with private industry
- Legislation ideas
    - Utilities—are there gaps in the law regarding utilities (e.g. National Grid/Eversource)?
    - There is no check on companies regarding their required encryption. There is a penalty, however, if a company has been hacked and it's found they didn't comply with encryption requirements
    - "Encryption on devices has become inhibitive"
    - Something to address vendors who charge $2000 to decrypt computers and mobile devices
    - M.G.L. chapter 266, Section 120 (unauthorized access to a computer system) needs to be updated to be more clear
        - CA, for comparison, is very aggressive at implementing statutory changes to criminal violations

- 2007 Cyber Crime Strategic Plan by the AGO—had a significant training component, encouraged information sharing
    - Training and information are still among the most important issues today

Dennis McDermitt, *Chief Information Security Officer & Chief Technology Officer*
Executive Office of Technology Services and Security (EOTSS)

- Dimensions of cybersecurity
    - Confidentiality
    - Integrity
        - Financial sector information
        - E.g. Swift Financial Network breached in 2017, $86M was stolen from Bangladesh
    - Availability
        - Russia's attack on Ukrainian power grid
        - Attack on major US internet provider; used thermostats to create DOS attack
        - Other "online assets" like cars, boilers ("all protected by the same 4-digit code"), wastewater treatment plants, etc. could be attacked
- "Bad guys" are after:
    - (1) Data (e.g. identity theft)
    - (2) Cybercrime—multidimensional
    - (3) Critical infrastructure—power, water, IT, elections
- Compliance does not equal readiness
    - Compliance – e.g. sending regular reports
    - Cybersecurity is dynamic
- Many people think (e.g. of utilities) that "they must be regulated" regarding cybersecurity. In fact, this is not the case. Currently cyber security is a patchwork of laws and regulations. It's not clear where state authority ends and private authority begins.
- Legislation ideas
    - "Critical infrastructure cybersecurity really scares me"
        - Recommended legislation regarding critical infrastructure

- Recommended the "new secretariat approach" to cybersecurity – attack your cyber infrastructure yourself.
    - Have someone try to break into your network
    - E.g. DHS sends out a scan/test for DHS computers weekly
    - Annual? Better if done on a continuous basis
- Regular testing of water and power utilities' cyber infrastructure
- Legislation to address weaknesses in online assets (e.g. cars, boilers, wastewater treatment plants, etc.)
- Centralize control of election infrastructure
    - Have not been able to engage Secretary of State office regarding election security

Appendix D – Meeting #3 Agenda

Agenda

1. Welcome
2. Guest Presentations
    a. 11:00am – 12:00pm: Brandon C. Brin, IT Director, Legislative Information Services.
        i. Opportunity for Q&A following the presentation
3. Discussion and Next Steps
    a. 12:00pm – 1:00pm: Discussion among Committee members regarding next steps and future speakers
4. Update from Previous Meeting Presentations
    a. Chris Kelly notified the Committee that he is researching the follow-up items provided to him after the meeting. He will share his research with the Committee upon completion.

Appendix E – Meeting #4 Agenda & Notes

Agenda

1. Discuss the scope of the committee's subject matter

a. Decide what to include
b. Determine what to exclude based on existing federal and state agency scope

2. Discuss potential regulatory requirements
    a. Prevention
        i. Testing
        ii. Training
        iii. Exercising
    b. Detection
    c. Response
3. Discuss responsibility/ownership – which existing/new agencies will have responsibility? Options:
    a. Create a new cyber regulatory agency
    b. Empower an existing agency with authority on cyber issues (e.g. EOTSS)
    c. Empower an existing agency with authority on cyber issues, but assign some authority to other relevant agencies
    d. Other?
4. Discuss next steps
    a. Develop a preliminary scope of the committee's subject matter
        i. Decide what to include
        ii. Determine what to exclude based on existing federal and state agency scope
    b. Assign responsibility/ownership
    c. Decide how proposed programs will be paid for

Notes

- Develop a preliminary scope of the committee's subject matter
    - Decide whether to include:
        - Critical state/municipality infrastructure
            - Agencies' computer systems
            - Agencies
            - Servers and databases

- Transportation
- Elections infrastructure

- Critical on-state infrastructure
  - Banking
  - Electric
    - The DPU already regulates electric, need to decide whether the DPU handles electric infrastructure cyber or whether another agency might handle cyber
  - Gas
  - Water
  - Telecomm
- Information privacy
  - Medical information
    - Healthcare industry
      - HIPAA regulates privacy here somewhat
    - Health apps and websites
      - E.g. is one's heart rate data secure?
  - Financial information
    - Banking industry
    - Banking apps and websites
      - E.g. mint.com
  - Public's computer/mobile device/cloud privacy
    - E.g. ransomware

- Decide whether to exclude based on:
  - What the federal gov't/federal statues already cover
  - What existing Massachusetts agencies already cover

- Potential regulatory requirements
  - Prevention
    - Testing (e.g. new secretariat approach to cybersecurity – attack your cyber infrastructure yourself. Have someone try to break into your network.)

        - Training (e.g. of state employees, private employees who have a hand in infrastructure
        - Exercising
    - Detection
        - Creating daily/weekly/monthly/annual procedures for detecting cyber-attacks and executing such procedures
    - Response
        - Developing a plan for responding to a cyber attack
- Assign responsibility/ownership. Decide whether to:
    - Create a new cyber regulatory agency
    - Empower an existing agency with authority on cyber issues
    - Empower an existing agency with authority on cyber issues, but assign some authority to other relevant agencies
        - Create a boundary between the cyber regulator and other relevant agencies
            - E.g. the cyber regulator, with each regulator's input, creates regulatory requirements for each industry and the relevant agency enforces/monitors their industry

Recommended questions to ask next speakers:

- Who are the current authorities on cybersecurity?
    - What agencies touch on cyber?
    - What is their scope?
- Who should be the authority on cybersecurity for:
    - Issuing regulations?
    - Holding private industry accountable for regulatory compliance?
    - Criminal investigation and prosecuting?

Appendix F – Cybersecurity Policy: Suggested Areas of Focus

Brandon C. Brin, *Director of Information Technology*
Legislative Information Services
November 8, 2017

Introduction

The following provides a brief overview of our suggested areas of focus, which the Special Senate Committee on Cybersecurity Readiness may be interested in exploring. This is by no means an exhaustive list, and aims only to identify areas that we have determined to be of significant importance given our limited expertise.

Consumer Awareness and Exposure Disclosure

Given the increasing incidence of cybercrimes such as identity theft and digital extortion (ransomware), a policy focus on consumer awareness with regard to the dangers of online fraud, personal information protection through social media, and good computing hygiene, may yield significant benefits. Consumers should be empowered with the tools necessary to protect themselves from cyber-threats.

Data Breach Reporting

Guidelines and policies should be developed on how data breaches and exposures are reported to law enforcement, regulatory agencies, and consumers. Focus should be spent on studying several of the more recent well-known data breaches, the manner in which those organizations responded to those exposures, and how customers were ultimately affected by those incidents. Entities should be discouraged from hiding or otherwise delaying notifications of data exposures to customers, as it deprives victims of the necessary information they need in order to take remedial steps to mitigate their exposure.

Cybersecurity in Schools

Public school curriculums should include or require coverage of cybersecurity related topics. This should begin at the first exposure to computers that students receive. This also happens to coincide with existing efforts to promote interest in science and technology subjects within schools. Further, supporting extracurricular activities within public schools such as hacking clubs, hack-a-thons, or otherwise any activity which promotes learning about cybersecurity should be considered. Such an addition would ensure that future generations would be adequately prepared for a world inherently more reliant on technology, while also developing an interest in those who may wish to pursue careers in cybersecurity, a field that is currently in high demand.

State and Municipal Organizational Training Requirements and Standards

Guidelines should be established for cybersecurity training within state and municipal government organizations for all staff members, particularly within organizations that conduct commerce or financial transactions, or those which own sensitive personal identifiable information.

Private Sector Training Requirements and Standards

201 CMR 17.00 established rudimentary guidelines requiring cybersecurity training for private sector entities which own or license personal information about residents of the Commonwealth. Without a means by which to measure and ensure compliance, it is difficult to say what effect, if any, that this policy has had on the overall security posture of private sector

entities. This policy should be further defined, in addition to exploring a strong method of enforcement to ensure compliance.

Private and Public Sector Engagement

Engagement with private and public sector entities for the purpose of facilitating information sharing, identification of best practices, and threat analysis yields significant benefits in increasing the cybersecurity posture across all organizations involved.

Cybersecurity Coordination

From a cyber and information security perspective, several state and municipal agencies currently have disparate responsibilities ranging from consumer awareness and protection, cybercrime investigation, to emergency preparedness. Short of tasking a single agency with all cybersecurity related responsibilities, coordination between all public and private sector stakeholders should be facilitated by a single entity, responsible for the following:

- Coordinate information sharing across all state and municipal agencies, collectively elevating statewide cybersecurity visibility.
- Assist and ensure state/municipal agencies with private sector engagement, specifically focusing on critical infrastructure providers, with the overall goal of strengthening the overall cybersecurity posture.

Enforcement for Personal Information Security Standards

As previously referenced, 201 CMR 17.00 established a solid framework for personal information security and data protection. These policies should be expanded upon, defining

industry specific regulations regarding personal information security. Engagement with affected industries may provide some visibility into the state of their current security practices, and what impact further regulation may have. An effective means of enforcement and determining compliance must be developed in order to ensure that these policies are adhered to, and to gauge their overall effectiveness.

Supporting Security Research

Currently, security researchers have no effective means by which to disclose discovered security vulnerabilities to entities or individuals without incurring some level of legal risk. Researchers should be empowered to notify individuals and organizations of potential vulnerabilities without incurring the risk of arrest or prosecution.

Empowering Law Enforcement

Ensure that law enforcement agencies have resources which they may call upon to advise or assist in response to computer or Internet based crime and threats. It would also be beneficial for officers to have cursory knowledge of basic cyber-crimes and how they function, specifically as they relate to fraud and harassment.

Empowering Investigators and Prosecutors

Given the distributed nature of Internet-based crimes, even if a responsible source has been identified it is often difficult to successfully prosecute those actors. Explore legislation which will give prosecutors the tools necessary to remove impediments to build successful criminal cases.

Critical Government Agencies and Infrastructure

As our reliance upon the Internet increases, it is important that we prioritize securing critical assets, and plan for the eventual scenario where they may become unavailable.

Private Sector Engagement Critical Infrastructure Providers: Preparedness

Given the significant role which these industries play in the functioning of society, critical infrastructure providers present valuable targets for attack. As such, it is imperative that we ensure the highest level of engagement with these entities to ensure that they are adequately secured, but also to maintain effective visibility over the current threat landscape.

Private Sector Engagement Critical Infrastructure Providers: Emergency Response

A significant component of engagement includes emergency preparedness, specifically emergency response plans which would be implemented post-cyberattack or disaster. These plans should be developed with input from all stakeholders (both private and public sector) and should establish baselines for actions which would take place following "worst case scenario" incidents. These plans should be tested and retested to confirm effectiveness, and periodically updated to address changing security concerns.

Coordination within Critical Government Agencies: Preparedness

Given the critical role which many state level agencies play in maintaining continuity of government, and their increasing reliance upon technology and the Internet for accomplishing their missions, it is imperative that all agencies are prepared by pursuing the following areas:

1. Interagency engagement relative to communicating cybersecurity strategies, experiences, and practices.
2. Establishing baseline security standards for all critical government agencies. (Example: NIST 800.)
3. Establishing training standards for all staff members within those agencies for cybersecurity awareness, with a specific focus on incident preparedness and response for key role-players within each organization.

Coordination within Critical Government Agencies: Emergency Response

Given the persistent nature of cyberattacks as compared to conventional emergency scenarios such as natural disasters, accidents, and terrorism, the eventuality of a successful attack having a significant impact on a critical government agency or resource is high. As such, it is imperative that those organizations share a similar framework for response plans to cyberattacks in the same fashion in which they share response plans for conventional emergency scenarios. These response plans should coincide with existing organizational emergency response plans, and address the following:

1. Common framework for cyber incident response across all agencies identified to serve a "critical" function for continuity of government.
2. Each agency should have disaster recovery plans or playbooks to prepare for the most common and worst case scenarios, including those relating to cybersecurity. These plans should be tested to validate effectiveness as well as specify expected service restoration time from the initial incident in question.

3. Action plans for inter/intra-agency communications during and post-incident. Many agencies are dependent upon Internet (email) and cell phone based technologies for primary communications, and may not be adequately prepared for scenarios where those services are unavailable.
4. Short and long term plans for maintaining operations during and after a cyber-incident where information technology resources may be unavailable or inaccessible.

Appendix G – Cybersecurity Committee Scope Proposal

Cynthia Stone Creem, *State Senator*
First Middlesex and Norfolk
November 17, 2017

At the November 8, 2017, meeting of the Special Senate Committee on Cyber Security Readiness, it was decided that proposals should be submitted to determine the scope of the Committee's work going forward. Cybersecurity is a very broad topic which touches upon many sub-topics. Therefore, bearing in mind the March 30, 2018, deadline of the Committee, Senator Creem submits the following proposal for the consideration of her fellow Committee members.

Committee Delegation of Pending Legislation

The twin topics of cybersecurity and consumer privacy are complex and recommending specific legislation is probably beyond the scope of this Committee, given our limited timeframe. Currently bills are scattered amongst more than half a dozen committees and this prevents the legislature from taking a coordinated approach to these topics. The Committee should consider whether a new committee should be formed or an existing joint committee should be expanded to be the centralized committee for cybersecurity and consumer privacy.

Cybercrime Investigation and Prosecution

Data breaches, hacks and other cybercrimes are becoming increasingly common and our constituents expect our public safety agencies to be able to pursue such criminals. The Committee should examine the extent to which Massachusetts public safety agencies have the resources and legislative tools they need to do this work. Such agencies could include Massachusetts State Police and Mass Chiefs of Police, MEMA, EOPSS, AG, etc. The Committee should also examine whether to create a new legal option for security researchers to disclose discovered vulnerabilities to the entities who should be aware of such vulnerabilities.

State Government Cybersecurity Functions Structure

The Committee should determine how each relevant state agency is currently managing cybersecurity and privacy functions in order to coordinate and simplify the delivery of services, resources, and information. Such coordination should reduce redundancies and ensure accountability. Such functions should include; interagency coordination, establishment of security standards, information sharing and resources for the private sector, security of voting systems and government databases, enforcement of state statutes and promulgation of regulations, consumer education, public school education, and STEM education.

Critical Infrastructure Preparedness

So many of our critical infrastructure systems are becoming increasingly reliant on technology and are therefore more susceptible to cyber threats. The Committee should examine the extent to which both Government Critical Infrastructure (DoT, DOER, DPU, DTC, Massport,

MBTA, etc.) and Private Sector Critical Infrastructure Providers (Energy, Transportation, Communications, etc.) are vulnerable to these threats and what more can be done to secure critical infrastructure, for example, regular vulnerability testing by an outside entity. This topic should also include an examination of emergency preparedness, specifically emergency response plans which would be implemented post-cyberattack or disaster.

State and Municipal Employee Cybersecurity Training

As the Committee has already heard, one common weakness in any organization is an employee falling for a phishing email or similar unsophisticated attack. The Committee should consider whether or not to mandate basic cybersecurity training for both state and municipal employees to both ensure that state assets are protected as well as to lead by example before requiring any training of the private sector. The Committee should also consider whether this training should also include sector-specific information on privacy laws, both state and federal, that are relevant to each agency's work (e.g. HIPAA).

Recommendation for Cybersecurity Committee Procedure

Due to the limited timeframe and breadth of topics contained in this proposal, the Committee should determine its scope as soon as possible. In order to increase the speed with which the Committee can gather information, topics for investigation could then be divided up between Senate offices so that fact-finding will take place between Committee meetings with each office reporting back to the group at general Committee meetings.

Appendix I – References

Blinder, Alan and Perlroth, Nicole. "A Cyberattack Hobbles Atlanta and Security Experts Shudder." *New York Times.* 27 March 2018. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

California Penal Code § 502

Campbell, Matt. In-person meeting. 16 November 2017.

"Crimes Against Property." *Massachusetts General Laws Chapter 266.*

"Current MA Agencies & the Scope of Their Cybersecurity Regulation." *Mass.gov.* www.mass.gov/dor/businesses/help-and-resources/licensing-and-regulation.html.

"Cyber and Grid Security." *Federal Energy Regulatory Commission.* 19 April 2018. https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.

"Cybersecurity Legislation 2017." *National Conference of State Legislatures.* 12 June 2017.

Dunietz, Jesse. "Is the Power Grid Getting More Vulnerable to Cyber Attacks?" *Scientific American.* 23 August 2017. https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/.

Garcia, Michael. "State Cybersecurity Strategies." *National Governors Association.* September 2016.

Gross, Michael Joseph. "Enter the Cyber Dragon." *Vanity Fair.* 5 September 2011. https://www.vanityfair.com/news/2011/09/chinese-hacking-201109.

Kelly, Chris. In-person meeting. 3 October 2017.

Knake, Robert. "A Cyberattack on the U.S. Power Grid." *Council on Foreign Relations.* 3 April 2017. https://www.cfr.org/report/cyberattack-us-power-grid.

Langde, Rohit. “WannaCry Ransomware: A Detailed Analysis of the Attack.” *Techspective.* 26 September 2017. https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/.

Lyford, Glen. In-person meeting. 17 November 2017.

McDermitt, Dennis. “Cybersecurity Readiness: A Brief Overview.”

Morris, David Z. “The Equifax Hack Exposed More Data Than Previously Reported.” *Fortune.* 11 February 2018. http://fortune.com/2018/02/11/equifax-hack-exposed-extra-data/.

“NERC Cybersecurity Standards.” *North American Electric Reliability Corporation.* 11 April 2013. https://www.nerc.com/news/Pages/NERC-Issues-Cybersecurity-Standards-Transition-Guidance-.aspx.

Newman, Lily Hay. “Github Survived the Biggest DDoS Attack Ever Recorded.” *Wired.* 1 March 2018. https://www.wired.com/story/github-ddos-memcached/.

“NIST Cybersecurity Framework.” *National Institute of Standards and Technology.* 16 April 2018. https://www.nist.gov/cyberframework.

Perlroth, Nicole. “A Cyberattack ‘the World Isn’t Ready For.’” *New York Times.* 22 June 2017. https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html.

Selyukh, Alina. “Every Yahoo Account That Existed In Mid-2013 Was Likely Hacked.” *NPR.* 3 October 2017. https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked.