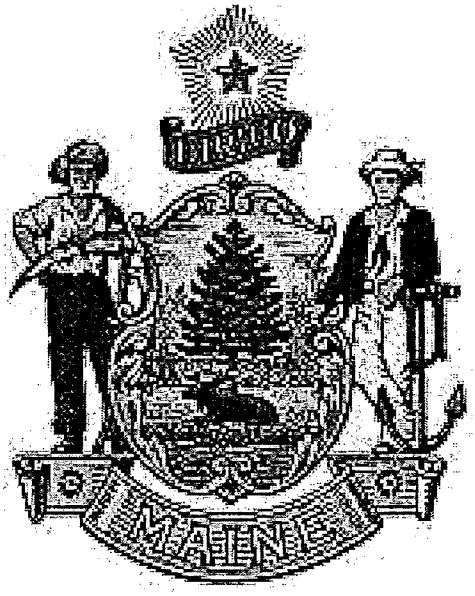
IMPROVING MAINE STATE CYBERSECURITY

Recommendations from the Governor's Information Protection Workgroup

December 20, 2016



On July 17, 2014, Governor LePage signed the Executive Order #2014-0003, launching the Maine State Information Protection Working Group. This Workgroup studied the overall Cybersecurity threat landscape, compared the current Maine State Cybersecurity posture with industry best practices, and arrived at a set of ten (10) recommendations to improve Maine State Cybersecurity

---

EXECUTIVE SUMMARY

The Governor's Information Protection Working Group studied the overall Cybersecurity threat landscape, compared the current Maine State Cybersecurity posture with industry best practices, and, especially, innovations in other states across the nation. The Workgroup arrived at a set of ten (10) recommendations, arranged around three primary themes: Stronger Defense, Proactive Stance, and Incident Response. The recommendations are listed below, and detailed individually in subsequent pages.

#	Recommendation		Theme(s)
1	OIT Cyber security Resource Allocation	Increase funding for OIT Cybersecurity to provide industry-standard Cybersecurity, including Vulnerability Scanning, Audit, Database Download Block, Workstation Access Control, Advanced Threat Detection, etc.	Stronger Defense Proactive Stance
2	PII Agency Protection	Fund the Agency Security Officer position for the seven agencies that transact heavily in Personally Identifiable Information.	Stronger Defense Proactive Stance
3	Position of the CIO	Elevate the CIO to a Cabinet-level position.	Stronger Defense Proactive Stance Incident Response
4	Expanded State Police Fusion Center and Computer Crimes Unit	Fund positions within the State Police Fusion Center and the Computer Crimes Unit in order to improve the capabilities of State Government to collect, analyze, and share intelligence and information on Cybersecurity threats, and to increase the State Police's capacity to conduct forensic analysis and investigations when a suspected Cybersecurity threat or attack has been committed within their jurisdiction, or against State Government.	Proactive Stance Incident Response
5	MEMA Cybersecurity Initiatives	Fund the MEMA Cybersecurity Coordinator.	Stronger Defense Proactive Stance Incident Response
6	Integrated Education Opportunity	Tighter Cybersecurity integration between the Colleges & Universities and the State government.	Proactive Stance
7	Continuity of Operations and Disaster Recovery	Fund Continuity of Operations (COOP) and Business Continuity - Disaster Recovery (BC/DR) planning, training, and exercise programs. Require all State agencies to develop and maintain COOP and/or BC/DR Plans. Require, at a minimum, all State agencies to conduct annual exercises of COOP and BC/DR.	Stronger Defense Incident Response
8	Maine National Guard	Fund the Maine National Guard for proactive Cybersecurity work even in the absence of disasters, as well as to respond to Cyberattacks on Maine assets.	Stronger Defense Incident Response
9	Local, Territorial, and Municipal Governments	Empower the CIO to provide Cybersecurity guidance to Local, Territorial, and Municipal Governments.	Stronger Defense Proactive Stance Incident Response
10	Critical Infrastructure	The Public Utilities Commission (PUC) should join the Governor's Information Protection Workgroup. PUC will also partner with other New England States to implement a New England Utility Cybersecurity Intelligence Center (NEUCIC).	Stronger Defense Proactive Stance

INTRODUCTION

Cyber probes and/or attacks against the State of Maine have increased five-fold in the last two years. Today, the Maine State network is probed more than 6 Million times a day, every single day. Of course, this is not a Maine-specific issue. Both the National Governor's Association[1] and the National Association of State CIOs[2] have made cybersecurity one of their top priorities.

Governor LePage's administration is acutely conscious of the importance of Cybersecurity, and is taking concrete steps to improve the Cybersecurity posture of the State. On July 17, 2014, the Governor signed the Executive Order #2014-0003[3], launching the Maine State Information Protection Working Group (the Workgroup). The group includes:

- State Chief Information Officer (CIO), (chairman)
- Chief Information Security Officer from th Office of Information Technology (OIT),
- Maine Emergency Management Agency (MEMA),
- Maine National Guard,
- U.S. Department of Homeland Security,
- University of Maine Security Director
- I.T. Director of the City of Auburn,
- I.T. Director of the City of Bangor

After its launch, the Workgroup also invited the I.T. Directors of the Legislative Branch, the Judiciary, and the Secretary of State to join the Workgroup on an ad-hoc basis.

The Workgroup has been meeting quarterly to examine threats and vulnerabilities, discuss risk management best practices, and provide policy recommendations. The final mandate of the Workgroup was to "present recommendations to the Governor and Cabinet".

---

[1] http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf

[2] http://www.nascio.org/Newsroom/ArtMID/484/ArticleID/296/Security-Tops-List-of-State-CIO-Priorities-for-2016

[3] http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1

THREAT LANDSCAPE

- Major threats to Maine's Cybersecurity include: crime syndicates motivated by money, hostile nations motivated by competitive advantage, "hacktivists" motivated by the desire to embarrass governments, and computer-savvy individuals motivated with a desire for publicity. Recent trends indicate that Cyberattacks are becoming more common and more sophisticated, and therefore, inflicting even more damage.

- Breach of citizen Personally Identifiable Information (PII) inflicts significant damage to a government, both in terms of costs to respond and mitigate, as well as the loss of trust from the public at large. According to the non-profit Identity Theft Resource Center[4], between 2005 and 2015, there were 5,810 PII breaches, exposing nearly 848 Million demographic records.

- According to a recent report[5] from the Government Accountability Office, Federal Cybersecurity incidents have jump 1,300% in the last 10 years.

- Over the last five years, more than 20 states have suffered Cybersecurity breaches, impacting more than 10 Million demographic records, with remediation efforts costing in excess of $100 Million.

  - ***State Level Breaches over the last five years:***

State & Agency	Reported	Impact
Illinois Board of Elections	July 2016	200,000 records
Washington Health Care Authority	Feb. 2016	91,000 records
Georgia Secretary of State	Nov. 2015	6 Million records
Texas HHS	Nov. 2014	2 Million records
Oregon Employment Database	Oct. 2014	850,000 records
Colorado Finance & Accounting System	Sep. 2014	300 users with access to Name, SSN, & Bank Account Number of state vendors
Tennessee Employee Benefits	Aug. 2014	60,000 records

(see Appendix A, for the full list of State Level and Non-State Breaches)

- Just in 2015-16, the following Maine-based businesses reported data breaches:

  - Common Market
  - Yellowfront Grocery

---

[4] http://www.idtheftcenter.org/
[5] http://www.gao.gov/assets/680/679877.pdf

- Jimmy The Greek's Restaurant
- Olympia Hotel Management / Brunswick Hotel
- Absolute Credit, LLC
- University of Maine
- Maine School Management Association
- Diman Regional Vocational Technical School
- Town of Brunswick Police Department
- Belgrade Regional Health Center
- Maine General Health and Subsidiaries
- Eastern Maine Healthcare Systems
- York Hospital Imaging
- Milestone Hospitality Management
- Anthem

According to the FBI[6], in 2015, there were 782 victims of Cybersecurity crimes in Maine.

[6] https://pdf.ic3.gov/2015_IC3Report.pdf

CURRENT STATE

The Maine State Executive Branch potentially holds the records of the entire Maine citizenry of 1.3 million people, including names, addresses, tax records, social security numbers, and vital records such as birth and death certificates. These records are spread across some 1,000 servers and some 2,000 applications. Many of these applications are open to the Internet, and increasingly, located in the cloud. Some 12,000+ knowledge workers access these records on a daily basis, often from personal and non-State devices. The Maine State network extends from Kittery to Madawaska, covering 400+ sites. Not only that, the network is shared with the Attorney General, the Secretary of State, the Judiciary, and the Department of Audit.

Ongoing Threats

- External probes and attacks have increased roughly five-fold in the last two years.

- The two biggest threats are
  - Well-organized criminal enterprises seeking demographic records, and
  - Targeted "phishing" emails to State employees.

- On an average workday, the State experiences about
  - More than 6 Million probes at its firewall
  - 30,000 generic spam emails
  - 100 spear phishing emails (i.e., specifically tailored to their targets)
  - 10 social engineering telephone calls ("Social Engineering" is the generic term where a targeted person is unknowingly led into subverting standard cybersecurity best practice. Includes everything from following somebody through a door without scanning their badge to looking over their shoulder while they type in their password.)
  - 15 workstations infected with malware. (Malware is the generic term for any agent that deliberately subverts the normal working of a computer.) On average, about six (6) hours of productivity is lost per infected workstation, which must be either disinfected or rebuilt.

- Episodic Attacks
  - May 2010: Up to a quarter of the workstation fleet hit with pornographic wallpaper
  - July 2014: The File Transfer system faced down 600,000 intrusion attempts per day, causing Denial-of-Service
  - October 2014: Up to 10 ransomware attacks per day. (Ransomware is a special kind of malware which encrypts files and demands ransom in order to decrypt those files.)
  - March 2015: Denial-of-Service attack against the Maine.Gov website. Site down for about 19 hours across two weeks.
  - From Time to Time: Website defacements

Cyber risk to Maine State (in descending order of likelihood):

Threat	*Explanation*	*Exposure & Mitigation*
Phishing: Targets employees. This is a tremendous exposure because the only protection against it is employees recognizing that the request is fraudulent.	Employee receives a legitimate-looking email that is really fraudulent, hunting for information.	***Exposure:*** Automated technologies block about 40% of email. Yet, hundreds of phishing emails get through. Unfortunately, tightening the filter further would block legitimate emails as well. Phishing attacks have been successful in multiple states (South Carolina, Texas, etc.) ***Mitigation:*** Each State employee is required to take the annual Cybersecurity training. Some agencies test their employees throughout the year. It is critical that all agencies with Personally Identifiable Information conduct the test multiple times a year.
Legacy software: Known vulnerabilities.	At some point, vendors stop supplying software 'patches' for their older systems. Attackers seek out these exposures and exploit them to breach the standard defenses.	***Exposure:*** The State network is 'probed' around 2.2 Million times a day by outside, automated agents, looking for vulnerabilities. ***Mitigation:*** Legacy software must be upgraded to keep current with vendor-supported versions. But, this is expensive.
Insider Threat: An employee or contractor with inside clearance deliberately steals information.	Often referred to as the Manning or Snowden effects, after two high-profile Federal cases involving Bradley/Chelsie Manning and Edward Snowden. Both stole large troves of Federal data.	***Exposure:*** Unknown at this time. ***Mitigation:*** Automated Data Loss Protection, Database Download Block, and Invasive Background Checks. None of them are widely operational right now.

Current Efforts to Combat Cybersecurity Threats

Defenses in Place

- OIT has a 12-person Cybersecurity team, spanning devices, applications, physical access, and the perimeter.
- Some 330,000 websites are blocked either because they contain inappropriate content or are known carriers of malware. Incidentally, Porn is one of the most prevalent vectors for malware.
- Annual Cybersecurity Training: Evidence indicates that training actually reduces the susceptibility to phishing, the single largest breach vector. In OIT's experience, agencies typically see a double-digit percentage drop in phishing vulnerability following completion of Cybersecurity training.
- OIT follows a process called Deployment Certification, which ensures that any new application going live is secure by using industry-standard tests to expose known Cybersecurity weaknesses in the code.
- OIT, MEMA, and the Fusion Center have jointly agreed on a Cybersecurity Incident Response Team (CSIRT), and a defined workflow. The CSIRT defines the workflow to respond to Cybersecurity incidents, including impact analysis, incident response, and communication.
- All OIT-managed devices have aggressive anti-malware.
- State email goes through aggressive spam filtration.
- Two Homeland Security devices monitor our external traffic and issue alerts for anomalies, vulnerabilities, etc.
- OIT works with Homeland Security and other commercial entities for third-party security audits.
- OIT has already rolled out Email Encryption enterprise-wide.
- OIT also offers extra capabilities on a per-agency basis, such as File Volume Encryption, Data Loss Prevention, Mobile Media (Thumb Drive, CDs, etc.) Encryption, etc.
- In June 2013, OIT and MEMA jointly hosted the first Maine Cybersecurity Summit. The purpose was to share information, best practices, gaps, and future directions. Participants included the Federal Homeland Security, the Maine National Guard, MEMA, the University of Maine OIT, and private industry.
- The CIO and the MEMA Director jointly send out a quarterly Risk Management newsletter. Also, the Chief Information Security Officer sends out ad-hoc threat advisories to all Executive Branch users, when appropriate.

Cybersecurity Insurance

- OIT modified the standard I.T. contracting rider to mandate Cybersecurity Insurance for cloud applications. The coverage is tiered, pegged to the number of Personally Identifiable Information records actually transacted as part of the contract.

- OIT, in conjunction with DAFS Risk Management, purchased Cyber Liability Insurance through AON, with the insurance carrier ACE. The policy covers the Executive Branch's internal hosted information assets and extends to the Office of the State Auditor, Treasurer, Secretary of State, Attorney General (network only), and the Judiciary (network only). The premium is $110,000 annually with a $400,000 deductible per claim. The policy is limited to $3 Million. The most important thing is that it provides access and referral to an independent panel of specialists in legal, incident management, forensic, consultation, and credit monitoring. It also assigns a Data Breach Coach to provide immediate triage, consultative and pre-litigation services in the event of a privacy event. The only caution is that any realistic breach will end up costing several times the current limit.

Two Executive Orders

- #2014-0003[7], dated July 17, 2014: Launched the Statewide Information Protection Workgroup, with the mandate to analyze threats, develop defenses, and report back to the Governor and the Cabinet. It also mandates annual Cybersecurity training to all Executive Branch Employees. It formally codifies the Cybersecurity Incident Response Team (CSIRT). Governor LePage has also directed OIT, MEMA and the Maine National Guard to work will all state departments and stakeholders to make sure that Maine's Cybersecurity preparedness and disaster recovery capabilities adapt to emerging threats, and adopt best practices from the public and private sector.

- #2015-0002[8], dated February 5, 2015: Bans pornography and sexually explicit material on State I.T. devices. Even incidental or off-duty hours are covered as part of the Executive Order. Pornographic internet sites are one of the most popular sources for malware, and prohibiting access makes a significant impact to Maine State Cybersecurity. Under this Executive Order, visiting pornographic websites becomes just cause for termination of employment. Of course, there is an exception when an employee's official duties require such access, and that includes Law Enforcement, the Maine Centers for Disease Control, et al.

Maine Breach Notification Law

- Maine Revised Statutes, Title X, Chapter 210-B, Notice of Risk to personal Data[9]
  - When a breach is suspected, the first test is whether the information is likely to be misused.
  - Notify within seven business days if notification does not hinder investigation.
  - Notify the Attorney General.
  - Notify consumer reporting agencies if more than 1,000 individuals involved.

---

[7] http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1
[8] http://www.maine.gov/tools/whatsnew/attach.php?id=638259&an=1
[9] http://legislature.maine.gov/statutes/10/title10sec1348.html

PARTNERSHIPS AND COLLABORATIVE EFFORTS

Current Partnerships

- We have created a strong Cybersecurity partnership amongst State Government, the University of Maine system and Thomas College, the Maine National Guard, U.S. Department of Homeland Security, the U.S. Coast Guard, and the Private Sector.

- Within the Executive Branch, OIT works very closely with MEMA and the Fusion Center.

- The Information Protection Working Group is making progress to better integrate the Attorney General, the Secretary of State, and the Judicial Branch technology representatives regarding Cybersecurity.

- Regular meetings amongst all parties, both formal and informal, for brainstorming and sharing of best practices.

- The University of Southern Maine Cybersecurity Lab is becoming a solid resource. And so is the Thomas College Security & Cyber Defense program.

- MEMA is working with Maine companies, organizations, and higher education to promote awareness and provide assistance to partners outside of State government for Cybersecurity responses statewide.

Joint Exercises

- 2012: Maine participated in the nationwide Cyber Storm IV exercise, testing capabilities of the Department of Labor, MEMA, OIT, and others.

- 2014: Cybersecurity was a key capability tested in the Vigilant Guard exercise, where Federal, State, County, and Local agencies were hit with reality-based attacks (fake USB drives, phishing attempts, denial of service, physical network infiltration, etc.)

- 2015: Senior Leadership Seminar and Tabletop Exercise for the Governor, the Cabinet, and senior Agency staff. The workshop was carried out by the Naval Postgraduate School's Center for Homeland Defense.

- 2015: The Maine Public Utilities Commission, along with other New England State Commissions, the various State Guard Units, and the Department of Homeland Security, participated in the Cyber Yankee exercise at Hanscomb Air Force Base.

- 2016: Maine participated in Cyber Storm V (CSV) in March 2016. This is a biennial national exercise conducted by the Department of Homeland Security. Facilitated by MEMA and OIT, participants also included DHHS, Education, the Fusion Center, and the Maine National Guard. Various Cybersecurity incidents (breaches, alarms, etc.) were simulated, and staff was challenged to identify, report, and respond to them. Participants included emergency managers, Cybersecurity technicians, business stakeholders, as well as public information

officers. CSV also featured the very first test of Maine's Cybersecurity Incident Response Team (CSIRT), a framework for collaborating on the response and public communication of a Cybersecurity incident. Besides the actual exercise participants and controllers, CSV also included observers from the Maine Public Utilities Commission, FEMA Region 1, and the State of Vermont.

- Numerous tabletop exercises and workshops conducted over the past five years with participation from all levels of government.