State Cybersecurity

> I[nformation] T[echnology] today is ubiquitous and is essential to virtually the U.S.'s entire infrastructure including dams, nuclear power plants, air-traffic control, communications, and financial institutions. Large and small companies alike rely on computers to manage payroll, track inventory and sales, and perform research and development. Every stage of the distribution of food and energy relies on IT. Western societies have spent years building this information infrastructure in ways that are interoperable, easy to access, and easy to use. Yet this open philosophy is also the Achilles' heel of the system.[1]

Cybersecurity plans attempt to provide a more perfect set of Hephaestus' armor for public systems and data. A complete cybersecurity policy maintains the confidentiality, integrity, and availability of electronic information and infrastructures. Availability is the ability to timely and reliably access data.[2] Integrity is the assurance that the data is both complete and accurate.[3] Confidentiality is the ability to limit access to data and to preserve privacy.[4]

The Department of Homeland Security has two goals in its cybersecurity plan: (1) creating a safe, secure, and resilient cyber environment; and (2) promoting cybersecurity knowledge and innovation.[5]

In addition to playing a role in the larger national puzzle, states must also address their

---

[1] Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 200 (2009).

[2] Idaho National Laboratory, et al., Cyber Security Procurement Language for Control Systems Version 1.8, ix (Feb. 2008), *available at* www.oe.energy.gov/DocumentsandMedia/SCADA_Procurement_Language.pdf

[3] Idaho National Laboratory, et al., Cyber Security Procurement Language for Control Systems Version 1.8, x (Feb. 2008), *available at* www.oe.energy.gov/DocumentsandMedia/SCADA_Procurement_Language.pdf

[4] Idaho National Laboratory, et al., Cyber Security Procurement Language for Control Systems Version 1.8, xii (Feb. 2008), *available at* www.oe.energy.gov/DocumentsandMedia/SCADA_Procurement_Language.pdf

[5] Department of Homeland Security, *Bottom-Up Review*, 23-25 (Jul. 2010), *available at* www.globalsecurity.org/security/library/report/2010/bur_bottom_up_review.pdf.

individual cybersecurity issues. The Multi-State Information Sharing and Analysis Center[6] leads the way in developing new state policies. Additionally, the National Cybersecurity and Communications Integration Center works to identify and warn states about threats to cybersecurity.[7]

States with comprehensive plans will need to deal with four main needs: (1) securing systems; (2) securing data; (3) developing knowledge; and (4) dealing with the aftermath of security breaches. Of course there is overlap between these four areas.

Securing Systems

"In an ever-changing technological environment, security controls that are state-of-the-art today may be obsolete tomorrow, while new security risks and emerging threats can occur at any time."[8] States need adaptable plans to deal with securing critical infrastructure, computer systems, and third party provider services.

The most pressing need is protecting critical infrastructure and process control systems such as the power grid. This type of cyber attack occurs less frequently than data theft; however, the potential consequences are much greater. This is an especially pressing need for states that have implemented smart grids.[9]

It is difficult to determine with precision the weakness inherent in critical infrastructure and

---

[6] www.msisac.org

[7] Office of the Press Secretary, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center* (Oct. 30, 2009), *available at* www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

[8] State Government Information Security Workforce Development Model A Best Practice Model and Framework 1, *available at* www.msisac.org/awareness.

[9] Jude Clemente, *The Security Vulnerabilities of Smart Grid*, Journal of Energy Security (June 18, 2009), *available at* www.ensec.org.

process control systems due to the danger of reporting vulnerabilities.[10] However, the Government Accountability Office found four factors contributing to the escalation of risks to these systems: (1) control systems are adopting standardized technologies with known vulnerabilities; (2) control systems are connected to other networks that are not secure; (3) insecure connections exacerbate vulnerabilities; and (4) manuals on how to use SCADA systems are publicly available.[11] Other groups such as The Tech Center at George Mason School of Law[12] are offering research in this area as well.

The Department of Homeland Security offers states free use of its Automated Critical Asset Management System in order to assess vulnerabilities in critical infrastructure.[13] This can be an important tool in developing state policy. DHS is also offering training funded by the National Infrastructure Protection Plan.[14]

State maintained servers, databases, and websites must be secured against internal and external threats, as well as negligence. There are a number of broad strategies that states can employ to mitigate security risks to these systems, including removing unnecessary services and programs, installing host intrusion detection systems, and limiting file and operating system permissions.[15]

---

[10] *See e.g.* Robert Lemos, SCADA Industry Debates Flaw Disclosure (June 16, 2006), *available at* www.securityfocus.com/new/11396.

[11] Idaho National Laboratory, et al., Cyber Security Procurement Language for Control Systems Version 1.8, vi (Feb. 2008), *available at* www.oe.energy.gov/DocumentsandMedia/SCADA_Procurement_Language.pdf

[12] www.cip.gmu.edu

[13] www.dhs.gov/ACAMS; www.dhs.gov/criticalinfrastructure

[14] www.dhs/gov/NIPP

[15] Idaho National Laboratory, et al., Cyber Security Procurement Language for Control Systems Version 1.8, 3-85 (Feb. 2008), *available at* www.oe.energy.gov/DocumentsandMedia/SCADA_Procurement_Language.pdf

In securing their noncritical infrastructure, states must make decisions about the type of system they wish to use. States have to decide between private self-controlled, private third-party controlled, and shared third-party networks. Each of these choices has advantages and disadvantages; therefore, most states will have some combination of all three. States must develop the duties of third party operators that own and/or operate much of the infrastructure. Generally, these duties are simply contractual. However, duties can also be imposed through statute, regulation, and industry standards.[16]

Data Security

"State and federal law require[s] state agencies to collect display, retain, destroy, and dispose of records that contain personal identifying information."[17] Federal privacy laws, including the Privacy Act of 1974, the Right to Financial Privacy Act of 1978, and the Health Insurance Portability and Accountability Act of 1996, place duties on states regarding personal identifying information.[18] These laws also require states that own or license personal information notify individuals of unauthorized access to that information.

States hold a tremendous amount of personal data and a responsibility to protect that data. This burden is likely to increase. The Global Information Security Workforce Study indicates that

---

[16] Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on Key Legal Trends*, 934 PLI/Pat 13, 21-24 (June - Jul. 2008).

[17] Idaho National Laboratory, et al., Cyber Security Procurement Language for Control Systems Version 1.8, 25 (Feb. 2008), *available at* www.oe.energy.gov/DocumentsandMedia/SCADA_Procurement_Language.pdf

[18] For more information on these laws *see* http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/federal-privacy.html.

a switch from protecting networks to protecting data is underway.[19] This switch is largely due to the realization that no network can every be totally secure, a fact illustrated by The National Security Agency's recent announcement that they consider their network compromised and now work on the assumption that hackers have the ability to invade their systems.[20]

In order to effectively meet the goal of protecting data, states have to constantly update firewalls, threat tracking, and system checks. Experts do not have any trouble agreeing what it is states need to do. Unfortunately they also seem to universally agree that what is required at this moment will be outdated in a matter of days or weeks. Thus it is impossible to develop static policies. Effective security must rely on teams constantly working to secure data. "[I]nstead of defining rigid, technologically-focused, temporally-limited legislative rules, perhaps we should be developing checks and balances – procedural and structural capabilities to ensure" data is not compromised.[21] These plans require physical facility and device security, access controls, intrusion detection, data integrity, confidentiality, and storage procedures, destruction and disposal policies, and audit controls.[22]

It should be noted that these measures will do nothing to protect the security of data that has been compromised through intentional or negligent conduct on the part of state employees. Instead

---

[19] Frost & Sullivan, White Paper, *The 2008 (ISC) Global Information Security Workforce Study*, 9-10 *available at* www.isc2.org/uploadedFiles/Industry_Resources/2008_Global_WF_Study.pdf.

[20] Brian Prince, *NSA: Assume Attackers Will Compromise Networks* (Dec. 17, 2010), *available at* http://www.eweek.com/c/a/Security/NSA-Assume-Attackers-Will-Compromis-Networks-395027/.

[21] Maeve Dion, *Privacy and Security: A Procedural and Structural Approach*, 4 The CIP Report No. 3, 15 (Sept. 2005), *available at* www.cip.gmu.edu/archive/cip_report_4.3.pdf.

[22] Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on Key Legal Trends*, 934 PLI/Pat 13, 50-51 (June - Jul. 2008).

states must have procedures in place to limit and track employees' access to data.

States cybersecurity plans should include duties on private parties that control data. Virtually every corporation has vast stores of data on individuals. States have a strong interest in protecting their citizens' data. This translates into a need to develop duties for corporations to protect data. A number of duties currently exist through statutes, regulation, common law obligations, rules of evidence, industry standards, contractual obligations, and even self-imposed obligations.[23] States must address the issue as to how they will impose on data holders the obligation to protect the information and data of their citizens.

Closely related to third party concerns are the issues raised by cloud computing. "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort."[24] Cloud computing can be very valuable; however, it has some risks not associated with general data storage. These include vendor security, a lack of information segregation, foreign data location, exposed interfaces, reputation sharing, and provider viability.[25] There is no checklist of decisions to be made before deciding whether and how to move information to a cloud. Instead each decision must weigh the risks and benefits individually by identifying the data risks, the potential cloud options, and the reasonableness of the risk inherent in the final decision.

---

[23] Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on Key Legal Trends*, 934 PLI/Pat 13, 21-24 (June - Jul. 2008).

[24] Peter Mell and Tim Grance, *The National Institute of Standards and Technology Definition of Cloud Computing* (Ver. 15 Oct. 7, 2009), *available at* csrc.nist.gov/groups/SNS/cloud-computing/

[25] Suzanne Bell, *Cloud Computing: Privacy, Data Security and Cross-Border Transactions*, 1010 PLI/Pat 125 (June 2010).

Information Technology Knowledge

It is imperative that states take up the cause of IT education as part of their comprehensive cybersecurity plan. The benefits will be three fold in that it will aid states by creating a future internal workforce, provide private sector jobs , and raise awareness among the general public.

Just as advances in technology are occurring at an exponential rate, so are advances in exploiting the emerging technologies; new technologies and new threats will be emerging *ad infinitum*. States must constantly adapt in their quest to protect themselves. Currently there are not enough experts to successfully develop and carry out cybersecurity plans. States have no choice but to create these individuals.

The State Government Information Security Workforce Development Model is a four-tiered IT workforce for state governments.[26] The model has one Chief Information Security Officer, three managerial areas, and a number of functional and generalists positions. This career path system is designed to internally build an effective workforce and create job satisfaction through advancement opportunities in order to aid recruitment and retention.[27]

In order to fill the pipeline with candidates, states have to develop technical school, community college, and university programs that produce educated candidates. In conjunction with the federal government, Maryland has set up the Center for Information Security and Assurance[28] which can serve as a potential model. This program offers degrees to a new workforce while doing

---

[26] State Government Information Security Workforce Development Model A Best Practice Model and Framework 1, *available at* www.msisac.org/awareness.

[27] *Id.*

[28] www.cisa.umbc.edu.

research that promotes cybersecurity advancements.

Cybersecurity education is also likely to create private sector job growth. The Global Information Security Workforce Study advises that the number of Information Security professionals will increase from 1.6 million in 2009 to 2.7 million by 2012.[29] States with educated workforces will draw employers seeking applicants with cybersecurity skills — a boon for economic growth as well as cybersecurity. States are already working with third parties for IT resources. Those relationships will continue to grow. The better able these third parties are to hire qualified security personnel the better security service they will be able to provide states.

Availability is an important component of any network; however, increased availability means more entry points for bad actors. While these entry points are largely designed for the ease and convenience of the public, an individual whose computer or access information is hacked may grant an intruder access to a broad array of confidential data.[30] For this reason, it is vital to the protection of infrastructure and data that states educate the general public.

Public education also protects individuals as they deal with private parties. Identity theft in the United States alone is responsible for economic losses of up to $50 billion annually.[31] It is widely believed that cybersecurity education is the best way to protect against identity theft.

Responses to Incidents

---

[29] State Government Information Security Workforce Development Model A Best Practice Model and Framework 1, *available at* www.msisac.org/awareness.

[30] Erin Kenneally & Jon Stanley, *Beyond Whiffle-Ball Bats: Addressing Identity Crime in an Information Economy*, 26 J. MARSHALL J. COMPUTER & INFO. L. 47 (Fall 2008).

[31] United States Congress, Committee on Ways and Means, *Facts and Figures: Identity Theft* (July 7, 2004), *available at* http://waysandmeans.house.gov/media/pdf/ss/factsfigures.pdf.

No cybersecurity policy or plan is going to stop every incident. Additionally, to the extent that security procedures are in place, we know that governments are failing to meet their own standards. For instance the 2010 General Services Administration audit found failures in at least four critical areas.[32] States must be prepared to respond to failures. In worst case scenarios this could be a shut down of the power grid. On the other end of the spectrum it might be the loss of confidentiality for a series of social security numbers. The federal government has adopted a National Response Framework to respond to catastrophes related to critical infrastructure.[33] The NIPP requires state and local governments to implement homeland security policies for protecting public safety and welfare, and ensuring the provision of essential services.[34] Currently these response and recovery plans are being enacted through regional public/private partnerships such as the Pittsburgh Regional Business Coalition for Homeland Security, the Pacific NorthWest Economic Region and Puget Sound Partnership, and the Potomac conference Emergency Preparedness Task Force. Partnerships such as these are logical due to the facts that critical infrastructure is in the hands of both public and private actors and the infrastructures of regions are tied together in ways which make them interdependent.

While states face the threat of a breach to their critical infrastructure, a more common cybersecurity breach occurs when businesses have a data breach. In 2003, California passed a data

---

[32] *GSA Falls Short in Four Critical Cybersecurity Areas* (Jan. 5, 2011), *available at* www.infosecurity-us.com/view/14956/gsa-falls-short-in-four-critical-cybersecurity-areas/; *see also Colorado Flunks Test of Its Information Security Systems* (Dec. 15, 2010), *available at* www.infosecurity-us.com/view/14702/colorado-flunks-test-of-its-information-security-systems

[33] Http://www.fema.gov/emergency/nrf.

[34] Dep't of Homeland Security, National Infrastructure Protection Plan (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

breach notification law which required possessors of data to inform consumers whenever their data was exposed.[35] As of 2010, 46 states have adopted some form of data breach law. Before 2003, the general consensus was that this was a type of enforcement that could only be handled by the federal government. The success of data breach laws demonstrated that states can take leadership roles in developing cybersecurity policies.

The most traditional approach to dealing with cybersecurity breaches is prosecution. The federal government already has a comprehensive series of laws dealing with known cybersecurity threats. There is an open question as to whether it is in states' interests to adopt their own cybersecurity criminal laws. In light of the strides made in data breach law following 2003, it seems that state experimentation in prosecuting cyber attackers is likely to have a positive impact on developing the law into a more effective tool.

[35] CAL. CIV. CODE § 1798.82