SECURITY IN THE ERA OF HIGH-TECH GOVERNMENT

Introduction to Public Administration - Final Assignment
By: Catherine Susman

Introduction

Technology has entered every aspect of our daily personal and business lives (Casper & McMillan, 2015, para. 2). We are living in the era of the "Internet of Things"[1] (IoT). Data originating from this new era is being captured, analyzed and stored in greater quantities than ever before (Watson, 2013, p. 15). In 2006, a study by Gartner Research found that data stored by businesses doubled every six months (Babcock, 2006, para 1). This storage and analysis will only continue to grow in the era of the IoT. The explosion of the IoT and related data threatens to overwhelm traditional security and information management techniques (Tully, 2015, para. 24). Government, like any business not only must learn to embrace the era of IoT, but also learn how to maintain security and privacy expectations in a world that is increasingly without traditional borders (Proctor, 2014, para. 2).

Specifically, this paper will explore the concept of technology; what it means to government including the concepts of e-governance;[2] cloud computing;[3] and other information and communications technologies (ICTs) and examine what actions government needs to undertake to manage the risk created by the use of technology and to maintain security and privacy in this new environment.

[1] According to Gallaugher (2014), the Internet of Things also known as "pervasive computing" is defined as "[a] vision where low-cost sensors, processors, and communication are embedded into a wide array of products and our environment, allowing a vast network to collect data, analyze input, and automatically coordinate collective action" (p. 77).

[2] E-governance is defined as "a general term used to describe the government's use of technology in performing its multiple responsibilities." (Holzer & Schwester, 2011, p. 465).

[3] According to Gallaugher (2014), cloud computing means "[r]eplacing computing resources – either an organization's or individual's hardware or software – with services provided over the Internet" (p. 89).

Background

In April 1965, Gordon Moore published an article in *Electronics Magazine* titled "Cramming more components onto integrated circuits" (Clark , 2015, p. A2). This article on chip manufacturing articulated the principle that became known as "Moore's Law" (p. A2). According to Gallaugher, Moore's Law provides "[c]hip performance per dollar doubles every eighteen months" (Gallaugher, 2014, p. 75). Over the next 50 years, this principle has allowed for the exponential growth of technology.

With the era of the IoT, technology entered its sixth wave[4] (Gallaugher, 2014, p. 76). All manner of common devices now have network connections. To fully understand how connected our lives are in the era of the IoT, it is helpful to look at some common devices many of use each day. Personal devices such as baby monitors, coffeemakers, security systems and door locks, activity trackers such as FitBit, and televisions are now "smart devices" in that they are connected through wireless networks and have the ability to track data related to your habits (Consumer Reports, 2015, p. 27). These devices are growing in use and popularity because the offer their users convenience and efficiency. In 2014, approximately 3.9 billion devices were networked (Tully, 2005, para. 10). This connection rate is expected to grow at approximately 35% per year. (para. 10). In the current year, 2022, it is estimated that there are 35 billion devices that are networked (G., 2022). This exponential growth of the IoT will be further fueled by new 5G technology.[5]

[4] The evolution of technology may be generally seen as having occurred in six waves: 1st wave – mainframe computers; 2nd wave mini-computers; 3rd wave personal desktop computing; 4th wave – internet computing; 5th wave – mobile devices; 6th wave – IoT (Gallaugher, 2014, p. 77).

[5] 5G technology is the fifth generation of wireless technology that provides faster speeds and greater bandwidth allowing for more connected IoT devices (Duffy, 2020).

The Problem

Unfortunately, the one of the main attributes that make the products attractive to users seeking convenience and efficiency, namely, the network connection, make those very products and the data they can track and store vulnerable to misuse by others (Consumer Reports, 2015, p. 24). Many of these devices, like many parts of the IoT, do not have well-established security protocols and even less protective security policies, resulting in more and more security breaches (p. 27). While recent trends and advances in technology are making IoT devices more secure, there are still substantial security implications (Marr, 2021).

There are far too many examples, within the last several of years, of breaches of personal devices, corporate data and government data. According to the Anti-Phishing Working Group, Inc. (APWG), a worldwide collation formed to respond to cybercrime, there was a record number of malware variants detected and an 18% increase in phishing[6] reports in the fourth quarter of 2014 (Anti-Phishing Workng Group, Inc., 2015, p. 1). Other more notorious and public breaches have occurred across industries. In the fall of 2014, government officials in the United Kingdom issued a public warning advising citizens that the live feed from many standard baby monitors and security cameras is readily accessible via the Internet (p. 27). In the area of education, in 2014, both the University of Maryland had a breach exposing 300,000 records and Indiana University had a breach exposing 146,000 records (Vaira, 2015, para. 1). In 2015, Rutgers University was hit with three cyberattacks during one

[6] Phishing is defined as "a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials." (Anti-Phishing Workng Group, Inc., 2015, p. 1)

semester (Kratovil, 2015, para. 2). In the retail industry in December of 2013, Target announced a security breach, a breach that would become the largest security retail breach in history (Riley, Elgin, Lawrence, & Matlack, 2014, para. 1). This one breach affected more than 40 million credit card numbers and 70 million customer records, and costs card issuers an estimated $200 million to cancel and reissue cards (krebsonsecurity.com, 2014, para. 1, 2, & 4). One of most disturbing breaches was to the United States Office of Personnel Management (OPM) breach publicly announced in April 2015. In this breach, actually two separate, although connected, breaches, resulted in the theft of personal information on 4.2 million former and current federal employees as well as the theft of personal data from another estimated 21.5 million individuals that were former, current or perspective federal employees or contractors (U.S. Office of Personnel Management, 2015, para. 1-2). Breaches and attacks, both large and small continue, as noted by researchers with Kaspersky[7] who estimated there were 1.5 billion cyber-attacks against IoT connected devices in the first six months of 2021 (Marr, 2021).

Cyber vulnerabilities, as shown in the above examples, occur generally in four areas: (1) Network; (2) Web/Internet; (3) E-mail; and (4) Mobile technology (Holzer & Schwester, 2011, p. 386). Security breaches in each of these areas continue to increase in number and scope. More and more it is becoming apparent breaches are not preventable, so a new solution to manage risk and protect security and privacy is needed (MacDonald, 2013, para. 21).

[7] Kaspersky is one of the world’s largest cybersecurity companies.

Identifying Causes

To some extent, the cause is easy to pinpoint, the pervasiveness of networked devices and the era of the IoT. Technology is everywhere and is part of every discipline (Gallaugher, 2014, p. 11). In an era of ever-increasing budgetary issues and waning trust in government, technology provides greater economy, efficiency, and access in and to government (Holzer & Schwester, 2011, pp. 380-381). Accepting the paradigm that technology use and the IoT will continue to expand due to the potential benefits, a careful examination of the current IT structure including risk management and security procedures most commonly employed is needed.

As technology usage has grown, industries have added policies and additional positions to help organize, coordinate and manage this area. For instance, all federal agencies now have Chief Information Officers (CIO) and many have Chief Technology Officers (CTO) (Holzer & Schwester, 2011, p. 383). These two positions are now being seen as essential not only at the federal level but also at the state and local level (p. 384). The rise in prominence of these positions correlates to the rise in prominence of and use of technology in government.

Shortly after taking office in 2009, President Obama commissioned a cyberspace policy review to assess federal structure and policies related to cyber and network security (U.S. Department of Homeland Security, 2009, p. iii). The issue of cybersecurity was identified as one of the key challenges that had to be faced (p. iii). The result of this assessment was the 2009 Cyberspace Policy Review report that concluded laws and policies in this area were an incomplete patchwork (p. 10). The report also concluded that successfully maintaining cybersecurity could not be done without collaboration across industries and governments (pp. 17-21). This report has become the foundation for federal government's actions on cybersecurity (U.S. Department of Homeland Security, 2015, para. 1). In partnership with APWG, the National Cyber Security Alliance (NCSA),[8] and the Online Consumer Security and Safety Messaging Convention,[9] the federal government launched a new campaign, *Stop.Think.Connect.*, in the fall of 2010 (U.S. Department of Homeland Security, 2015). In 2013, President Obama issued Executive Order 13636 "Improving Critical Infrastructure Cybersecurity." This order covered three key areas including critical infrastructure, policy coordination, information sharing on cybersecurity as well as acknowledgement to ensure coordination regarding privacy and civil liberties protections.

To compete in today's marketplace, government continue to use and embrace technology and the IoT. However, as shown from all the breaches, there is a critical need for managing security and risk in this cyber environment. The central issue, therefore, is ensuring protocols around risk and cyber security keep pace with the development of technology (Proctor, 2014, para. 5).

Setting Objectives

Prior to launching a particular security approach that can keep pace with technology, government must first determine what it needs to and desires to accomplish (Holzer & Schwester, 2011, p. 139). The objective in this case may seem obvious, but it is

[8] NCSA is a non-profit public-private partnership whose mission "is to educate and therefore empower a digital society to use the Internet safely and securely at home, work and school, protecting the technology individuals use, the networks they connect to and our shared digital assets." (National Cyber Security Alliance, 2015). NCSA has board members from Google, VISA, Microsoft, AT&T, Bank of America, McAfee, Comcast, and Intel. (National Cyber Security Alliance, 2015).

[9] Online Consumer Security and Safety Messaging Convention is a coalition of non-profit entities and government formed to develop messaging for the general public to encourage safer online habits. The results of this coalition are the *Stop.Think.Connect.* campaign (PR Newswire, 2010).

ineffective to assert a vague objective such as keeping the government’s systems and information safe. For meaningful objectives around which to build an effective policy, the objective must be: (1) specific; (2) measurable; and (3) answer the “who, what, how much, when, and where” (p. 139).

With respect to data and information security, a 2009 worldwide study found that only 33% of respondents maintained an accurate inventory of the location of their data assets and only 24% maintained an accounting of who had access to those data assets (Gallaugher, 2014, p. 329). Given the breaches that have occurred in both private and public organizations, it is reasonable to suggest that the public sector is not ahead of corporations on tracking and securing its data assets. The first step is performing an inventory of the data assets of the organization. This inventory will allow the determination of where the data is, who has access to the data, and the degree to which that data is critical/confidential (p. 329). Once this inventory is performed, government may create its objectives around the security of its data assets.

The first objective is to secure the critical/confidential data by ensuring the data is segregated on servers/network, access to and use of the data is carefully and continuously monitored, and access to the data requires authentication (Vaira, 2015, para. 1). The second objective is to secure the sensitive, but non-critical data, by ensuring access to and use of the data is monitored and access to the data requires authentication (Gallaugher, 2014, p. 330). The third objective is to promote transparency in government by allowing public access to non-sensitive data by ensuring the data is accessible via the Internet as well as continued traditional methods of access

(Holzer & Schwester, 2011, p. 381). In reviewing the above three objectives, all three are seen as "must" objectives in that they are necessary (p. 139).

Evaluation of Alternatives to Achieve the Objectives

To evaluate the alternatives, it is important to note that cybersecurity is seen as having three components: (1) Deterrence; (2) Detection; and (3) Defense (Holzer & Schwester, 2011, p. 386). These three components are also referred to as: (1) Prevention; (2) Detection; and (3) Response (Vaira, 2015, para. 4). The deterrence/prevention component is focused on taking actions to prevent a breach from occurring (para. 5). Prevention includes the deployment of firewalls,[10] keeping software current and patched,[11] and password and user authentication requirements (para. 5). The detection component focuses on identifying potential cyber threats and includes a variety of methods to identify unauthorized access or problematic behavior (Gallaugher, 2014, p. 330). The last component, defense/response, focuses on having a pre-formulated incident response type plan designed to limit the damage and recover from the breach (p.331). In reviewing alternatives to meet all three of the objectives, it is also important to remember the objectives are about keeping data/information secure, not necessarily about prevention of attacks or breaches (MacDonald, 2013, para. 5). Lastly, it is important to remember not all data assets need to be maintained with the same level of security (para. 13). While an approach to cybersecurity needs to include all three components, the emphasis on those components and how they are implemented varies.

[10] Gallaugher (2013) defines a firewall as "[a] system that acts a control for network traffic, blocking unauthorized traffic while permitting acceptable use" (p. 330).

[11] Merriam Webster's dictionary defines parch as "a minor correction or modification in a computer program" (Merriam-Webster Dictionary, 2015).

Three alternative options will be explored in this paper to assist in determining the best approach to meeting the above-listed objectives.

First Alternative: The first alternative to meeting the objectives is through a focus on prevention of breaches and cybersecurity incidents. Traditionally, prevention is the prong most commonly emphasized. The four areas of prevention security commonly implemented are: (1) Physical safeguards; (2) System safeguards such as firewalls and passwords; (3) Encryption and data transfer security measures; and (4) Policies and procedures regarding access and use of information (Holzer & Schwester, 2011, p. 469). Each of the four areas is utilized primarily to prevent a security compromise. The success of each of these four areas depends on the extent of control the organization and its information technology (IT) staff have over the network, the servers, the applications, and the end users (Proctor, 2014, para. 2). Increasingly, however, the control of an organization and its IT staff is weakening (para. 5). The increase in cloud computing and mobile devises and access means IT staff are not able to exert the control necessary to maintain a security program focused primarily on prevention (para. 6). This control is further hampered by the nature of government which is to be transparent and open to the greatest extent possible (Holzer & Schwester, 2011, pp. 469-470). In order for government to maintain transparency, it cannot operate in a walled garden.[12] For government to meet its mission, it must operate in an open and collaborative environment. It is, therefore, not feasible to expect government and its staff to refrain from open cyber activities. As such, government needs to have a

[12] According to Gallaugher (2013), a walled garden is defined as “a closed network or single set of services controlled by one dominant firm” (p. 189).

security policy that includes deterrence/prevention as a key component while recognizing the need for transparency.

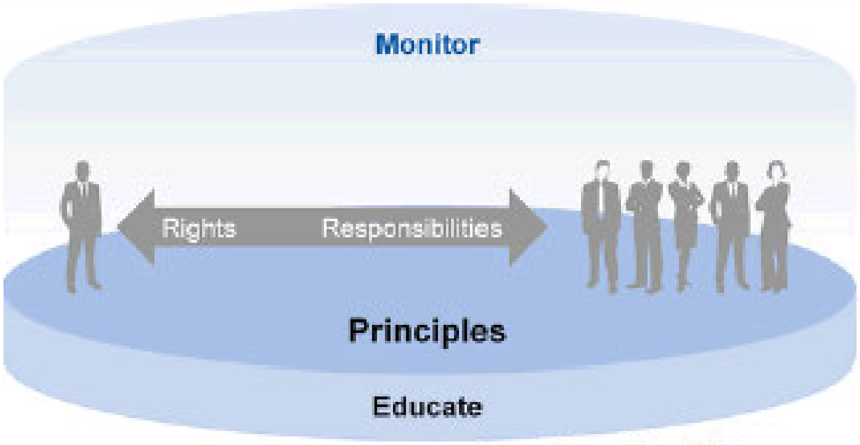
Second Alternative: The second alternative focuses on the detection component. This focus would allow the recognition of the continued loss of control over the networks, servers, operating systems, and applications (MacDonald (2013), para. 4). This approach also allows the security of the information to be the focus of the security policy (para. 5). Under this approach, pervasive monitoring and rapid detection are the focus. This focus will allow users the freedom needed to take advantage of technology and will allow more openness and transparency, while continuing to keep information safe (para. 21-24). A real-world example of the benefits of pervasive monitoring is the Target breach. In that example, all losses experienced in the Target breach could have been prevented due to monitoring that identified the breach prior any data being lost (Riley, et al., 2014, para. 8).

Third Alternative: The last alternative is to focus the cybersecurity and the security of data assets in a defense/response mode. If the increase of attacks and breaches is assumed, then this is clearly a critical component of any cybersecurity policy. This component will help ensure losses from a breach are limited as much as possible (Vaira, 2015, para. 9). This approach also allows for better resiliency of the organization in preventing a shut-down (para. 9). Further, when paired with detection, this component may assist in preventing the spread and damage of any breach. Again, using the real-world example of the Target breach, the monitoring detected the breach prior to data loss, but Target had no defense/response to such notice. Target did not respond until after until the one of the largest breaches of data in retail history had occurred (Riley, et al., 2014, para. 5). Target thus serves as a cautionary tale of the need for a defense/response plan. As the main focus of a cybersecurity policy, however, a primarily defensive strategy is not the best strategy for meeting all the objectives and protecting the data.

The Preferred Alternative

While employing all three security approaches, prevention, detection, and response, is critical in a cybersecurity policy, the focus of such policy should primarily be on detection rather than prevention. Further detection should be coupled with a strong, thorough response plan for the best protection. The following diagram illustrates the best structure for meeting all three objectives:

Figure 3. People-Centric Security



Source: Gartner (April 2014)

(Proctor, 2014, para. 27).

References

Anti-Phishing Workng Group, Inc. (2015, April 29). *Phishing Activity Trends Report 4th Quarter 2014.* Retrieved August 4, 2015, from APWG Unifying the Global Response to Cybercrime: http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf

Babcock, C. (2006, January 9). *Data, Data Everywhere.* Retrieved August 4, 2015, from InformationWeek.com: http://www.informationweek.com/data-data-everywhere/d/d-id/1039328?

Casper, C., & McMillan, R. (2015, January 5). *Agenda Overview for Security and Risk Management Leaders, 2015.* Retrieved August 4, 2015, from Gartner, Inc.: https://www.gartner.com/doc/2954530?ref=SiteSearch&sthkw=cyber%20security&fnl=search&srcId=1-3478922254

Clark , D. (2015, April 18-19). Turning 50, Tech Axiom Moore's Law Shows Age. *The Wall Street Journal*, pp. A1-A2.

Consumer Reports. (2015, June). In the Privacy of Your Own Home. *Comsumer Reports, 80*(6), pp. 24-26.

Consumer Reports. (2015, June). The Machines Are Watching. *Consumer Reports, 80*(6), pp. 27-30.

Duffy, C. (2020, March 6). What is 5G? Your questions answered. *CNN Business*. Retrieved March 2022, from https://www.cnn.com/interactive/2020/03/business/what-is-5g/index.html?msclkid=d3773313a72211ec8f8d357564f00e61

G., N. (2022, March 14). How Many IoT Devices Are There in 2022? [All You Need To Know]. *techjury*. Retrieved March 2022, from https://techjury.net/blog/how-many-iot-devices-are-there/?msclkid=98f7a9c8a6e911ecbbc491e62dc0da64

Gallaugher, J. (2014). *Information Systems A Manager's Guide to Harnessing Technology* (Vol. 2.0). Washington, D.C.: Flat World Knowledge, Inc.

Holzer, M., & Schwester, R. W. (2011). *Public Administration An Introduction.* Armonk, New York: M.E. Sharpe, Inc.

Kratovil, C. (2015, May 4). *Latest Cyber Attack Slams Rutgers For Four Days Straight.* Retrieved August 6, 2015, from New Brunswick Today: http://newbrunswicktoday.com/article/latest-cyber-attack-slams-rutgers-four-days-straight krebsonsecurity.com. (2014, May 14). *The Target Breach, By the Numbers.* Retrieved August 4, 2015, from Krebs on Security: http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

MacDonald, N. (2013, May 30). *Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence.* Retrieved August 4, 2015, from Gartner, Inc.: https://www.gartner.com/doc/2500416?ref=SiteSearch&sthkw=Prevention%20is%20Futile%20in%202020%3A%20Protect%20Information&fnl=search&srcId=1-3478922254

Marr, B. (2021, December 13). The 5 Biggest Internet Of Things. *Forbes*. Retrieved March 2022, from https://www.forbes.com/sites/bernardmarr/2021/12/13/the-5-biggest-internet-of-things-iot-trends-in-2022/?msclkid=98f89370a6e911ecb024c61c3c5dba80&sh=932f3ae5aba0

Merriam-Webster Dictionary. (2015, July). *Patch*. Retrieved August 7, 2015, from merriam-webster.com/dictionary: http://www.merriam-webster.com/dictionary/patch

National Cyber Security Alliance. (2015). *StaySafeOnline.org About Us*. Retrieved August 6, 2015, from StaySafeOnline.org: https://www.staysafeonline.org/about-us/

Obama, B. (2013, February 12). *Executive Order - Improving Critical Infrastructure Cybersecurity.* Retrieved August 4, 2015, from The White House Office of the Press Secretary: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

PR Newswire. (2010, October 4). *Stop.Think.Connect. Broad Government, Industry, and Non-Profit Coalition Unveils First-Ever Coordinated Online Safety Message.* Retrieved August 6, 2015, from PR Newswire: http://www.prnewswire.com/news-releases/stopthinkconnect-broad-government-industry-and-non-profit-coalition-unveils-first-ever-coordinated-online-safety-message-104282618.html

Proctor, P. E. (2014, April 10). *Digital Business Forever Changes How Risk and Security Deliver Value.* Retrieved August 4, 2015, from Gartner: https://www.gartner.com/doc/2706021?ref=SiteSearch&sthkw=Digital%20Business%20Forever%20Changes%20how%20risk&fnl=search&srcId=1-3478922254

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 13). *Missed Alarms and 40 Million Stolen Card Numbers: How Target Blew It.* Retrieved August 4, 2015, from Bloomberg Businessweek: http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Tully, J. (2015, February 27). *Mass Adoption of the Internet of Things Will Create New Opportunities and Challenges fro Enterprises.* Retrieved August 4, 2015, from Gartner, Inc.: https://www.gartner.com/doc/2994817?ref=SiteSearch&sthkw=Mass%20Adoption%20of%20the%20Internet%20of%20Things%20Will%20Create%20New%20Opportunities%20and%20Challenges%20for%20Enterprises&fnl=search&srcId=1-3478922254

U.S. Department of Homeland Security. (2009). *2009 Cyberspace Policy REview.* Retrieved August 4, 2015, from U.S. Department of Homeland Security: http://www.dhs.gov/publication/2009-cyberspace-policy-review

U.S. Department of Homeland Security. (2015, June 29). *Overview of Stop. Think. Connect.* Retrieved August 4, 2015, from U.S. Department of Homeland Security: http://www.dhs.gov/stopthinkconnect-overview

U.S. Office of Personnel Management. (2015, July). *Information about OPM Cybersecurity Incidents*. Retrieved August 4, 2015, from opm.gov: https://www.opm.gov/cybersecurity

Vaira, P. F. (2015, May 19). *Protecting Against Cyberattacks on Colleges and Universities.* Retrieved May 2015, from The LEgal Intelligencer: http://www.thelegalintelligencer.com/id=1202726786359/Protecting-Against-Cyberattacks-on-Colleges-and-Universities?slreturn=20150423180002

Watson, H. J. (2013, January-March). All About Analytics. *International Journal of Business Intelligence Research, 4*(1), pp. 13-28.