Cybersecurity Challenges to American State and Local Governments

Donald Norris, Anupam Joshi and Timothy Finin
University of Maryland, Baltimore County, Baltimore, Maryland, USA
norris@umbc.edu
joshi@umbc.edu
finin@umbc.edu

Abstract: In this paper, we examine cybersecurity challenges to American state and local governments. In particular, we address the extent and magnitude of cyberattacks against these governments, the problems these governments face in preventing attacks from being successful, the barriers internal to their organizations that make cybersecurity difficult to achieve, and actions that they believe should be taken to improve cybersecurity practice. Our research method consisted of a focus group of information technology (IT) and cybersecurity (CS) officials from one American state. Among other things we found that cyberattacks, mostly in the form of malicious emails, are constant, 24/7/365, and can number in the tens of thousands per day (at least among state government and larger local governments). The participants in our focus group noted that while they weren't perfect at it, they felt that for the most part they had the technical side of cybersecurity under good control. These governments' biggest cyber challenge is human error; that is, end users who (mostly by mistake and without malice) open an attachment or click on a link in a phishing email that then allows an attacker into the government's IT system. We also found that the probability of a successful phishing cyberattack is relatively high. These governments face several barriers when attempting to prevent cyberattacks and when endeavoring to mitigate successful ones, including: insufficient funding and staffing; problems of governance (namely, lack of control over all actors within a governmental unit due mainly to the federated nature of government); and insufficient or under-enforced cybersecurity policies. Our participants also noted that there are several common sense ways that state and local governments can improve cybersecurity. Among others, these include: frequent vulnerability assessment, continual scanning and testing, securing cybersecurity insurance, improving end user authentication and authorization, end user training and control, control over the use of external devices (flash drives, etc.), improved governance methods, sharing information about cyberattacks and cybersecurity policies and practices among governments, and, finally, creating a culture for cybersecurity in governmental organizations. Areas for further research into state and local government cybersecurity include: the types of cyberattacks that state and local governments typically face; the types of actions that these governments should take to prevent the attacks from being successful and to mitigate the results of successful attacks; gaps between these governments' need to prevent and mitigate cyberattacks and their ability to do so, including barriers to effective state and local government cybersecurity and best cybersecurity practices; and recommendations for improving state and local government cybersecurity.

Keywords: cybersecurity, cyberattack, local government, state government

1. Cybersecurity challenges to American State and local governments

The issue that we examine in this paper is that of cybersecurity at the state and local government level in the United States. This is an increasingly important issue for at least the following reasons. First, there are 50 state governments in the U. S., and according to the U S. Census Bureau (2014), there are more than 90,000 units of local government in United States, including nearly 39,000 general purpose governments (of which 3,031 are county governments, 19,519 are municipal governments and 16,360 are town or township governments. Nearly all of these governments have critical information technology (IT) systems and cumulatively spend billions of dollars each year to support them. Second, these IT systems are vulnerable to cyberattack and, indeed, many, especially those in state governments and larger local governments, are under constant attack, experiencing in the order of 10,000 attacks per day or more (Focus Group, 2013). Third, the IT systems in these governments, especially the larger ones, contain large stores of personally identifiable information or PII as well as other sensitive information and, of course, access to governmental funds.[1]

Fourth, in 2014 alone, cyber criminals succeed in penetrating the websites and roaming around in the IT systems of large private sector organizations in the U. S. like Home Depot, Target, JPMorgan Chase, AT&T, Yahoo, E-Bay, Google, Anthem and numerous others. In addition, public sector organizations like the U. S. Central Command, the U. S. Postal Service, the White House, the National Oceanic and Atmospheric Administration and the University of Maryland, College Park also suffered successful cyberattacks. In some cases, millions of individuals were affected as elements of their PII (name, address, drivers' license number, credit card numbers, social

[1] Today, cyber criminals seek PII perhaps more than any other single item in order to impersonate individuals whose identities have been stolen and then to use those stolen identities to steal money and goods

security numbers, health information and the like) were stolen. Even worse – undercover police officer information, jail information. Moreover, the number of cyberattacks grows annually.

Fifth, cyberattacks have moved from being a nuisance to something very serious and are deployed by only by state actors, but also by sophisticated transnational, non-state actors such as terrorists and financial criminals. Finally, cybercrime is very costly to the U. S and world economies. McAfee (2014) estimated that cybercrime costs the world economy more than $400 billion annually, and the cost of cybercrime continues to increase.

The World Wide Web presents one of the most commonly used vectors for attacks. This attack vector can be divided into two major components. One is the fact that many companies and governmental organizations set up web sites to provide information and services online. In some cases, especially for government, this information is legislatively mandated. For governments also, web presence is tied to e-governance -- providing citizens with online access to information, government services, and interaction with government personnel. Such web sites, which will typically have data driven backends (hard drives, servers, and the like that contain the organization's data) and forms to accept input, can be attacked using a variety of "injection" attacks, where cyber criminals attempt to place malware or malformed input into a backend to cause it to run specific code. A good example of this is SQL injection attacks, where the database of the government that contains its information is attacked.[2]

The second major attack vector component is the use of Internet enabled technologies, especially social media, email and mobile apps. To attack specific targets, "spearphishing" is increasingly used. Publicly available information (from websites, social media sites like Facebook, and even public records) is gathered to build the profile of a person, and then email messages are crafted that are very specific (for example, from a person's college friend talking about a proposed reunion and providing a link). These tempt a person to click on that link, which in turn installs malware on their computer.

For these reasons, it is important to understand the cyber threats that state and local governments face, their current efforts to both protect their IT systems from attack and to mitigate after a successful attack and the barriers they face in mounting these efforts. This understanding will allow us to make recommendations for improved local government cybersecurity.

2. Method

In order to begin to address the issue of cybersecurity among American state and local governments, we conducted a focus group in late 2013 that included information technology (IT) and cybersecurity (CS) professionals from the state government and several local governments in our home state of Maryland. These included the Chief Information Officer (CIO) of the state of Maryland (pop. 5.8 million), who had also been the state's Chief Security Officer(CSO) and the CIO or the CSO of the City of Baltimore (pop. 631,200), and the Maryland Counties of Baltimore (pop. 806,100), Howard (pop. 288,500), Montgomery (pop. 975,600), and Prince George's (pop. 865,600). Thus, we had access to IT and cybersecurity professionals who literally are on the front line of fighting cybercrime in one American state. As we will show throughout this paper, their knowledge, expertise and experience were incredibly valuable to our research.

Four of the local jurisdictions represent the greatest concentration of population in the state, and two of them (Howard and Montgomery Counties) are the wealthiest in the state and among the wealthiest in the nation. This is important to note because research over at least the past four decades on information technology in local government has revealed that adoption of information technology, especially innovative technology, is related to local government size and resources (Norris and Reddick, 2013; Coursey and Norris, 2008; and Norris and Kraemer, 1996). Although the sample of governments in our focus group is too small and unrepresentative for us to be able to generalize from it, the findings are nevertheless heuristically valuable and have formed the basis for further cybersecurity research that we are currently conducting. In the following pages we discuss the most important findings from this focus group meeting.

3. Findings

We asked the participants a number of questions, beginning with the extent and magnitude of cyberattacks that they experienced, and also included questions about the problems they face in preventing attacks from being

[2] SQL stands for Structured Query Language and is the standard language for managing relational database systems (Wikipedia, 2015).

successful, the barriers internal to their organizations that make cybersecurity challenging, and actions that they believe should be taken to improve cybersecurity practice at the state and local level.

4. Attacks

We asked the focus group participant show frequently their sites were attacked. In response, they asked us what we meant by attack. There ensued a discussion among the group and the researchers that led to a consensus that today most attacks are made against a government's public facing website or via email; most attacks involve social engineering and phishing rather than direct attacks on firewalls; and attacks number in the tens to hundreds of thousands or more every day.[3] This is a 24/7/365 event. However, as one participant noted, "…but, you know what? We've come to the point where we don't characterize those events as attacks. They're routine."

We asked the participants if the technical side of cybersecurity was especially problematical for them. They said that, while they weren't perfect at it, they felt that for the most part they had the technical side of cybersecurity under pretty good control. As one participant said: "We know that we block a huge amount. We know that some of the things we block, our users want to have come through and some of the things that we would like to block come through anyway." Another participant estimated that in his county, about 40 percent of emails were blocked. And this means that "…you're in the hundreds of thousands if not near a million a month that we're just blocking and [are] not even making it to the end user."Recent studies (Securelist, 2014) estimate than over 65 percent of all email is spam. While much of it is merely unwanted advertising, a significant fraction is sent as an attempt to get the recipient to open or download a malicious attachment or to be enticed to provide valuable personal information such as account information.

The participants unanimously agreed that the end user is the principal problemthey face in being able to maintain a high level of cybersecurity. One participant said: "And our biggest struggle now is…the human being, our weakest link." The crux of the matter is that inevitably, a member of their organization will download an attachment or click on a link sent in an email phishing attack and that allows an attacker into the local or state government's IT system. This happens mainly as a result of human error – the end user should have known better than to click on the link, but clicked anyway. Participants also noted that the phishing attacks are getting more sophisticated and less easy to readily identify as such. They also reported that malice occasionally occurs among end users, for example, in which one end user would attack another end useron the system or an end user would engage in fraudulent activity within the city or county government's IT system.

In one case reported by a participant, two government employees out of 10,000 inadvertently opened a malicious URL. And, as this participant noted, while two out of 10,000 is statistically impressive, the damage was nonetheless done as the attacker got into the system. According to Verizon's2013 Data Breach Investigations Report, the likelihood of a phishing attack succeeding is quite high.[4] Here, the report asked how many email messages would it take to get a single user to click on a malicious attachment.

> *It's pretty easy to see why [phishing]…is a favored attack…and the answer to our question is "three." Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click. Run that campaign twice and that probability goes up to 80%, and sending 10 phishing e-mails approaches the point where most attackers would be able to slap a "guaranteed" sticker on getting a click. To add some urgency to this, about half of the clicks occur within 12 hours of the phishing e-mail being sent (p. 38).*

We also asked who the perpetrators of the attacks were and the participants told us that attacks come from across the globe. However, as the 2013 Verizon report found, most attacks come from within a relatively few nations, with China (30 percent), Romania (28 percent), the U.S. (18 percent), Bulgaria (seven percent) and Russia (five percent) totaling 88 percent of identified attacks.

Next, the participants noted that most of the attacks are automated. "These people are literally setting up complex systems and letting it just hit global to see what they can get." Additionally, they agreed that the attackers mostly were criminals rather than, for example, young people breaking into systems for sport, political

[3] Phishing is use of email in which the attacker, posing as a trusted source – someone the victim knows personally, attempts to gather PII and other sensitive information. The attacker's phony email will contain a link that the attacker wants the intended victim to open, thus allowing malware to enter the victim's computer and harvest information.

[4] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

activists or terrorists. One participant put it this way: “The perpetrators are looking for opportunity…Primarily it’s financial opportunity. These people are thieves.” The participants said that the attackers want PII in order to impersonate their victims for financial gain. One participant agreed, saying: “So, yeah, there’s a lot are other causes for it, or there is lots of other motivations. There is espionage, there is notoriety, there is revenge, but money is on the top of the list and it is the lion’s share of why this occurs.”

Participants noted that other risks from cyberattacks, including three of particular concern. First, there is a risk of having an agency’s computers compromised and subsequently used as part of a botnet controlled by the attackers, which can then be used to launch attacks on other computers.[5] A second risk mentioned was that a compromised computer or account in one agency can be used to try to gain access to a related agency that may have valuable information or control important assets. For example, a compromised computer in a county parks department might be used to launch an attack on a state database and from there try to gain access to a federal computer system. Fourth, some local and state agencies are responsible for maintaining critical cyber-physical infrastructure systems such as traffic and water utilities. Attackers who gain access to these could potentially do a great deal of harm.

5. Barriers

We next asked about the barriers that state and local governments face in the area of cybersecurity. The major barriersthat they reported included:

- insufficient funding and staff
- governance and federation (executive, legislative and judicial branches and divisions within the executive)
- insufficient or under-enforced cybersecuritypolicies

Funding and Staffing: Insufficient funding and staffing are closely related. Without adequate funding it is difficult for state and local governments (or any organization) to provide the needed level of cybersecurity protection and to hire and retain qualified IT and CS staff. Lack of funding and staff are also among the top barriers reported in surveys of IT and e-government among U. S. local governments since the 1990s (Norris and Reddick, 2013; Coursey and Norris, 2008; and Norris and Kraemer, 1996).

One participant noted that the IT budget in his county equaled

> *“…less than two percent of the overall budget. Less than two percent. Yet 100 percent of the people in [the county] are using IT. So, you know, you’re right, you know, we don’t have the resources, we don’t have the manpower. [We]… try and use our money the best way we can and…you’re right, sometimes things can be solved with money.*

Insufficient funding has increasingly led local governments to investigate alternative ways of handing cybersecurity, including outsourcing. One county represented on this focus group reported that its programs and data were already 90 percent running on cloud computing infrastructure. This transfers much of the responsibility of securing the data and services to the cloud service providers for whom it is a central part of their business. Others noted that they are beginning to view cybersecurity as a commodity or a service that they purchase on the market. One of the advantages of this, in addition to potential cost savings, as one participant put it, is: “Google has 2,000 security engineers…I’ve got four.”

On somewhat of a discouraging or pessimistic note, the participants agreed, however, that even with greater funding and more staff, their systems will continue to be attacked and will probably, eventually, be a victim of a successful attack. Therefore, there is a need not only to continually harden the IT infrastructure, but also to have in place a recovery plan in the event of a successful attack. This is so because, in case the systems go down, there is the need for continuity in government.

While this is certainly true, a different participant cautioned that overdoing recovery plans might not be such a good idea after all. He put it this way: “So but what would happen to us if our system went down. I mean the

[5] A botnet is a collection of computers connected to the Internet that have been infected with malicious software that allows them to be controlled remotely. Botnet can be exploited without the knowledge of their computer's owners for many illegal purposes including sending spam email, engaging in click fraud, launching distributed denial of services attacks, bitcoin mining or stealing private information (Stone-Gross, et al., 2009). The U. S. Federal Bureau of Investigation (FBI) estimated that the GameOver Zeus botnet comprised over one million computers in 2014 (FBI, 2014).

world is not going to end. We are not Amazon. We're not Google…That [the IT system] is not the crux of our business." The business of local government, to which he was referring is service delivery, most of which would continue in spite of a loss of IT services. Moreover, several participants said that they were not terribly worried about having their information exfiltrated since most of it is public data.[6]

Governance: One of, if not the main, reason for the governance problem with respect to cybersecurity is that state and local governments are federated among executive, legislative and judicial branches. The IT department (ITD) or function is typically located in the executive branch but it has no authority over the legislative and judicial branches, which are constitutionally and legally separate in the American system of government.[7] As one participant put it: "I've got responsibility over all three branches of government. However, I can't legally enforce policy, due to the pesky constitution, over the legislative and judicial branches. But I am responsible for their security."

A second important governance issue is that, even within the executive branch, there are often departments or units that have "special protection" and remain outside of the purview of the ITD. Police departments and other units were mentioned as entities that were the "favorites" of elected executives and, therefore, were granted special dispensation from oversight by the ITD and its cybersecurity policies and regulations.

A third governance issue is differences among departments within the executive branch. One participant put it this way:

> *"And well, even within the executive branch we've got 35 different departments, each with varying levels of risk tolerance. So being able to enforce a policy on department X versus department Y is vastly different depending upon what their leadership thinks is important to them. And what their mission is. Recreation feels like they have to provide services for ball fields and for swimming pools, etc., etc., that's what their mission is but then…you start thinking about the millions of dollars that they get in credit card transactions every year and that then becomes a big potential security risk."*

A fourth governance issue, noted by another participant, is that at least in some governments there are multiple networks to manage. In this participant's government, "… there are eleven, I stopped counting at eleven, different data networks, eleven different data networks. Over the years, well-meaning people patched weird connections to them that we may or may not understand and we're trying to untangle that..."

Policy: Many cybersecurity vulnerabilities originate with the risky behavior of an users, such as choosing insecure passwords, failing to keep their computer's software updated, downloading attachments from unknown email correspondents and publishing personal information online. Organizations combat these problems by training their workforce on cybersecurity best practices, defining security policies and implementing procedures to enforce them. As one participant put it: "There has to be someone in charge [and]…there has to be policy…the rules of the road." Unfortunately, not all state and local governments or units within them have appropriate cybersecurity policies and not all implement the policies that they have well. A common example is not enforcing rules that require users to get cybersecurity training. "Well, as far as security awareness is concerned, our struggle it getting it to be mandatory." Another participant, however, noted that in his county, "The county executive backed it up. People had to come to training centers." The take away here is that governments need rigorous cybersecurity policies, especially around user training and the dos and don'ts of user behavior and those policies need to be stringently implemented and enforced.

6. Actions to improve cybersecurity

Finally, the participants listed a number of actions that they believed should be taken to improve state and local government cybersecurity, including:

- Assess vulnerabilities–We asked whether these governments did, in fact, formally and continually assess their cybersecurity vulnerabilities and the response was that most did so, but only on an on ad hoc basis, and conducted more of an audit than a formal assessment.

[6] In cybersecurity contexts, exfiltration is the unauthorized release of data from within a computer system, typically done by malicious software that has been installed on the system.

[7] In certain types of county governments and in council-manager forms of municipal government. The executive and legislative functions are combined. However, the judicial branch of government remains separate.

- Consider cybersecurity insurance – Cybersecurity insurance is intended to mitigate losses from cybersecurity incidents such as data breaches, business interruption and network damage (DHS, 2014). One participant noted that local governments across the nation are beginning to buy such insurance and commented that, at least as of the date of the focus group meeting, this insurance was relatively inexpensive. Acquiring such insurance also affords a local government the opportunity to conduct a formal risk assessment, because doing is part of the insurance application process for these programs.
- Two factor authentication and authorization -- This is also a policy issue and would require all users to have to enter two separate factors in order to sign on to the IT system, say a password and a pin. Some participants strongly supported "two factor auth" (as it is often called), but other noted that it was expensive and intrusive on users who don't like it.
- User training and control– See above discussion about the end user problem.
- Control over external devices – Users inadvertently upload dangerous files to the governmental unit's IT system through personal flash drives, tablets, smart phones and the use of Dropbox. Policy lags behind the use of these devices and needs to catch up.
- Overcome the governance/federation problem – Here policy and practice need to address the separation of powers and provide appropriate authority to IT and CS officials to enable them to exercise control over all IT assets for which they are responsible.
- Create a culture for cybersecurity – This would be a culture in which all parties, especially end users, but also elected officials, understand the need for excellent cybersecurity, are trained in it, practice it, and are held accountable. As one participant noted, it is about being aggressive, not passive, toward cybersecurity.
- Continually scan and test– This was really the only technical recommendation made by the participants and it means to be constantly aware of cyber threats, to scan for them continually, to scan for vulnerabilities and to test the capabilities of the system to prevent and recover from cyberattacks.
- Share information among organizations – Here participants noted that there is a lot of information about cybersecurity, especially information about threats and best practices. Indeed, there is so much information, one participant noted, that the sheer amount could be overwhelming. Therefore, he suggested the creation of a clearinghouse would be able to collect information, triage it and would know how to and to whom to circulate it.

7. Conclusion and future research

The results of this focus group with expert state and local government IT and cybersecurity practitioners in one American state found that the computer systems of their governments are under constant cyberattack and that attacks range in the tens of thousands or more per day. Indeed, cyberattacks are now so common that they viewed by these practitioners as "routine." We also found that at least some cyberattacks will inevitably be successful, if only because of the sheer number of attacks and the high mathematical probability of their success.

A particularly important finding of this research is that it is not the technology side of the cybersecurity equation that is most problematical for state and local governments. Instead it is the human element – people are the weakest link.[8] By this, the participants meant that either because of carelessness, lack of training, lack of attention to training or (rarely) malice, some government workers will inevitably take actions that will compromise cybersecurity. The most common among them is to open a dangerous URL or file attachment.

Barriers to more effective cybersecurity among these governments included principally money, staff, governance and policy. There is insufficient funding for cybersecurity and for sufficient cybersecurity staff among the governments represented. Hence, they find it difficult to provide the levels of cybersecurity that this challenge demands. Governance is an issue because of the federated nature of state and local government where one unit within a government may have responsibility for cybersecurity but not the commensurate authority to mandate cybersecurity. Additional governance concerns included departments with special

[8] Two of the authors of this paper (and leaders of the focus group) are computer scientists and the third is a political scientist. All three of us entered into preparation for the focus group meeting with the assumption that the principal cybersecurity problem would turn out to be the technology (hardware and software). The computer scientists can be forgiven this assumption. This is the world in which they live. The political scientist cannot be forgiven for this assumption, however, because his own research and a great deal of social science research into IT and government, have shown the critical role that "orgware" (the people and processes within organizations) play in IT use, success or failure. So, the best he can do is to apologize for this lapse and promise to remember it in future research.

protection, varying levels of risk tolerance and large numbers of networks to be managed. Finally, policy is a challenge because many governments wither have poorly developed policies or are unable to implement the policies that they have, including policies mandating end user training and policies preventing untrained users from accessing IT assets.

Last, the participants identified nine different recommendations to improve cybersecurity at the state and local government level. Since we discussed these in the previous section, we will not repeat them here. However, we will note that all but two of the recommendations (assess vulnerabilities and continually scan and test) were directed toward the orgware versus the technology side of cybersecurity.[9]

As we noted earlier, because this focus group was conducted among a few IT and cybersecurity officials (albeit expert practitioners) in a single American state, our findings cannot be generalized. However, based on comments made by the participants, we suspect that these findings will resonate with state and local IT and cybersecurity officials around the nation if not also around the world. These findings also suggest the need for further and more in-depth research into state and local government cybersecurity, which based on our review of the literature, is currently not the subject of many systematic studies. Further, such research should be directed to at least the following areas:

- The types of cyberattacks that state and local governments typically face and, thus, the types of actions that these governments should take to prevent the attacks from being successful and to mitigate the results of successful attacks;
- Gaps between these governments' need to prevent and mitigate cyberattacks and their ability to do so, including barriers to effective state and local government cybersecurity and best cybersecurity practices; and
- Recommendations for improving state and local government cybersecurity.

Such research could be undertaken using several different methods, including surveys, case studies, additional focus groups, and the quantitative analysis of large sets of state and local cybersecurity data, if and when such data sets may become available. We urge researchers, however, not to worry a great deal about methods at this point, but to get with the task of conducting state and local government cybersecurity research that is theoretically sound and of practical use to state and local governments.

References

Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime.* A report prepared for the Center by McAfee (June 2014). Accessed September 21, 2014 at: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Coursey, D. and Norris, D.F. (2008). Models of e-government: Are they correct? An empirical assessment." Public Administration Review. 68(3): 523-536.

Department of Homeland Security, Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues, National Protection and Programs Directorate, July 2014

Norris, D.F. and Reddick, C.G. (2013). Local E-Government in the United States: Transformation or Incremental Change?Public Administration Review.73(1).

Norris, D.F. and Kraemer, K.L. (1996). Mainframe and PC computing in American cities: Myths and realities. *Public Administration Review*, *56(6),* 568-576.

Shcherbakova, T., Vergelis, M. and Demidova, N. (2014) (November).Spam and phishing in the Q3 of 2014. *Securelist.* (http://securelist.com/).

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R.,Kruegel, C., and Vigna, G. (2009).Your botnet is my botnet: analysis of a botnet takeover. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*. November 9-13, 2009. Chicago, IL.

U. S. Census Bureau. 2012. *2012 Census of Governments*. Accessed February 8, 2015 at: http://www.census.gov/govs/cog/

U. S. Federal Bureau of Investigation. 2014. *GameOver Zeus Botnet Disrupted.* Accessed February 13, 2015 at: http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

Verizon. 2013. 2013 Data Breach Investigations Report. Author. Accessed January 21, 2014 at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Wikipedia, 2015.*SQL*. Accessed January 29, 2015 at: http://en.wikipedia.org/wiki/SQL

[9] Orgware consists of the people and processes in an organization that interact with the technology (the hardware and software).