Technology Trends to Prepare for in 2015

By Rob Roque

2015 is expected to be an exciting year for technology, including cybersecurity, wearable technology, social media, 3D printing, cloud computing, and predictive analysis.

In 2014, cyber hacks and data security became a weekly, and sometimes daily, occurrence in the popular news. 2015 is likely to bring more of the same — along with a greater focus on cybersecurity. But 2015 is also expected to be an exciting year for technology in general. This article highlights a few of the predicted trends, along with insight into potential policy implications.

CYBERSECURITY

The software security company, McAfee, estimates that hacking costs businesses between $300 billion to $1.4 trillion annually.[1] Although this represents just 0.5 to 1.5 percent of the global gross domestic product, recent hacking appears to be more sophisticated than in the past, and the severity of the incidents is growing. But is the weakness really in the technology? Although all of the incidents involved computer intrusions, many of the vulnerabilities had nothing to do with software or hardware design. For example, major news organizations reported that the widely reported November 2014 Sony hack (when confidential employee data were publically released) was started by a former employee with deep knowledge of the company's servers and where data were located. Similarly, in September, the Federal Aviation Administration learned about employee-related security weaknesses when a disgruntled contractor destroyed servers, precipitating the shutdown of air traffic control near Chicago, one of the world's busiest air sectors. Any quick research of recent hacking incidents will reveal that most security vulnerabilities stem from humans.

As technology becomes more prevalent in business operations, the public sector should not only assess its software and hardware vulnerabilities, but its employee vulnerabilities as well. An assessment should begin with an inventory of systems and a determination of where data are housed. Next, consider which employees have access to critical systems and what access they have to data. Thorough background checks for new employees (even for employees that change positions within the organization) should be considered. Finally, organizations should have a policy in place for prohibiting access to technologies once an employee has separated from the organization.

WEARABLE TECHNOLOGY

Wearable technology, ranging from cameras on police vests to health sensor bands, will be prevalent in 2015. The devices are popular because they provide consistent, objective observations of the surrounding environment, and we can expect to see them used more as ways of managing risk and delivering transparency.

Cameras in police squad cars have already proven effective, and wearable cameras are the next trend. The public sector will need to consider these types of devices for liability purposes, and it will also need to look at ways in which the devices affect personnel policies and employee contracts. It has been argued that people behave in a more positive manner when they are aware of a wearable device, whether it is a citizen reacting to a police officer or a police officer engaging a suspect. This phenomenon has increased the popularity of the devices, and some police unions have reacted positively to wearable cameras. Organizations that are considering a wearable camera policy don't necessarily need to be worried about controversy, since the wearers may benefit from the technology as much as the subjects being captured by the camera.

Governments may also need to consider policies related to other types of wearable technologies such as health monitoring devices in 2015. The Affordable Care Act allows employers to offer greater incentives for healthy behavior. Health-care technology experts have said that health insurance providers are likely to provide enticements to individuals leading healthy lifestyles, or to charge more to individuals who are not.[2] Organizations may need to consider these devices as part of their overall health programs since one day participants may be able to lower premiums based on active monitoring. As with the awareness engendered by the wearable cameras, employees who actively monitor their health may change lifestyle habits to achieve positive reporting results.

Managers should monitor and update any policies that are affected by the use of wearable devices, and such policies may need to be incorporated into employee contracts. Multiple police departments have implemented wearable device programs, so policies already exist that can be examined and customized for your organization. Employee health monitoring in the public sector is rare, so sample policies may need to be obtained from other industries. In either case, consult your human resources professional and general counsel when developing these types of policies.

As technology becomes more prevalent in business operations, the public sector should not only assess its software and hardware vulnerabilities, but its employee vulnerabilities as well.

SOCIAL MEDIA AND ONLINE PRIVACY

Communications devices and social media outlets are ubiquitous, providing ways for individuals to share their thoughts and opinions on a global scale. Ironically, there are also social media sites that cloak communications. Social media is not going to go away anytime soon, and public-sector organizations should acknowledge that they exist and that there are positive aspects to their existence. But at the same time, there should be a good strategic reason for their existence within the organization.

Some employers research social media sites before hiring employees. Disciplining employees for social media posts can create problems, unless the post breaches safety or security policies. Some organizations restrict access to social media sites while employees are at work, but IT administrators must keep in mind that doing so may not be a good strategy if your organization communicates to its constituents through social media sites or if employees rely on social media for professional development, best practice guidance, or peer-to-peer networking.

Organizations are most vulnerable to temporary posting sites, which allow users to exchange messages that auto-delete after a set period of time. SnapChat, an application that is typically used for social communications, allows users to share messages and videos. More clandestine communications are offered through services such as Wickr. These services allow users to send encrypted messages that are not stored on any server, and each transmission is scrambled differently. This kind of tool offers limitless possibilities for security breaches.

Although it is not an encompassing solution regarding social media, legal experts advise employers to develop employee policies regarding the use of technology (including personal devices) in the workplace as well as providing guidance to employees regarding social media postings. The National Labor Relations Board provides some guidance, but it is best to consult legal experts specializing in

employee use of social media before developing a policy.

3D PRINTING

This technology is one of the most exciting developments in recent years. 3D printing permits the user to build tangible, three-dimensional items from software with relatively cheap and readily available hardware. Using technology that has its roots in inkjet printers, a user can replicate items ranging in car parts to human parts, allowing users to be machinists and biomedical engineers. 3D printing can be particularly important to local governments, potentially making it possible to build replacement parts for assets when the supplier no longer exists.

Issues that may be associated with 3D printing include trademark compliance, safety, and security. Intellectual property issues such as patent and trademark infringement should be considered. Also, since 3D printing does not entail the same manufacturing processes in the duplication process, the quality of the 3D printed item may not be as good as the original. Finally, it may be possible to use 3D printers to fool biometric readers, such as fingerprint readers, by creating a thin duplicate of a fingerprint.

THE INTERNET OF THINGS AND COMPUTING EVERYWHERE

The Internet of Things is defined as the environment where devices are networked and interact with each other. It is estimated that 9 billion devices have this function today. By 2020, the number of connected devices is expected to be 24 billion.[3] Connected devices enable televisions to share recorded programs, jet manufacturers to monitor any jet engine in flight, and copying machines to e-mail staff when ink levels are low.

> Wearable devices are popular because they provide consistent, objective observations of the surrounding environment, and we can expect to see them used more as ways of managing risk and delivering transparency.

"Computing Everywhere" can be difficult to understand. It is a term coined by a technology research firm, and it refers to the ubiquity of computing devices — that is, human interaction with computing devices is natural, requiring little effort or thought. Automatically uploading a picture from your smartphone to your favorite social media device is just one example of this process. In some organizations, employees are expected to collaborate electronically, to take notes electronically, and to consider technology not as a tool but as a natural extension of themselves.

Of course, more connected devices mean more security concerns. Expect to see more emphasis on security that guards software, hardware, and the network infrastructure. Organizations will need to rethink their technology policies and develop comprehensive strategies related to the prevalence of technology. The National Institute of Technology Standards has developed a framework that addresses technology security in this environment.[4] It is written from a business perspective and can easily be understood by non-technical staff. Despite the risks associated with device interconnectivity, organizations should take advantage of this trend because the benefits and efficiencies of being interconnected far outweigh any risks associated with securing infrastructure.

PERSONAL TECHNOLOGY

According to the Pew Research Center, the majority of Americans own and use personal technologies.[5] Almost three-quarters of all smartphone users have accessed their phones in the past month to access information they needed immediately, such as Internet data, meeting collaborations, or for research. Personal technology will be even more pervasive in the future.

The public sector will need to accommodate these devices. Organizations that issue personal devices should consider policies that address assignment responsibilities and what to do if a device is lost or damaged. Organizations that allow employee-owned personal devices in the workplace will also need to develop policies on the use of these devices and the workplace data that is allowed to be handled by them (if any). These policies should address the data and security process and not specify devices, since personal devices will change over the years. It is too difficult to predict what a "personal device" will be defined as in the future.

CLOUD COMPUTING

According to PC World, approximately 90 percent of all businesses use some form of cloud computing.[6] Numbers are more difficult to find for state and local governments, but one cloud service claims more than a 1,000 organizations in 49 states.[7] The next year will see more sophisticated cloud offerings since more applications will be available through the cloud. Traditional cloud services, such as online storage, may dwindle as customers choose to keep data in-house. Offerings such as application management, infrastructure management, and disaster recovery may be more attractive as cloud offerings, since applications are becoming more complex. As a result, hybrid cloud offerings — where part of the technology resides in the cloud and the other part resides at the customer facilities — may become commonplace. Managed services will also become more reliable.

PREDICTIVE ANALYTICS

Predictive analytics, which is more accurately described as "predictive computing," uses past trends to improve the user's experience — think of a smartphone that displays weather information wherever the user is, and also the weather at the user's destination and the estimated time of travel, no data entry required. In this example, the phone has recorded past commuting patterns and used that data to predict the information the user will need.

Predictive computing is often mistakenly lumped into the world of forecasting, but in fact it uses technology to improve surrounding environments, based on past trends. Imagine conference rooms being automatically cooled or heated in time for meetings. Meeting times are obtained from the organizer's online calendar. Similarly, imagine assigning snow plows based on weather data, traffic conditions, and past traffic patterns. This is what predictive computing is all about — mastering historical data to gain future efficiencies.

> Public-sector organizations should acknowledge that social media exists — but there should be a good strategic reason for its existence within the organization.

Organizations should strive to support employees that are willing and able to work with predictive analytics tools and predictive computing. Governments will benefit from staff members who are able to proactively deal with potential issues based on trend analysis. Expect to see more sophisticated applications as data become more readily available and consumed.

CONCLUSIONS

There is a principle in technology called Glass' Law, which states that for every 25 percent increase in the functioning of technology, complexity increases by 100 percent. In accordance with Glass' Law, modern enterprise systems have required more IT resources to run successfully. Modern systems, for example, rely on the Internet, leverage data from legacy systems, and integrate with desktop applications. The underlying technology infrastructure required to make this happen is complex. The cost for this type of infrastructure is also complex since software providers seldom offer a simple licensing formula. Given that the Internet of Things and Computing Everywhere will continue to grow, expect more complex technology infrastructure. This means that those in charge of implementing technology and those in charge of financing technology will need to collaborate if they expect to build a successful long-term strategy for their enterprise technology.

Notes

1. The Economic Impact of Cybercrime and Cyber Espionage, McAfee Center for Strategic and International Studies, July 2013.
2. Parmy Olson, "Wearable Tech Is Plugging into Health Insurance," Forbes, June 19, 2014.
3. Om Malik, "Internet of things will have 24 billion devices by 2020," October 13, 2011, GigaOm.com.
4. Framework for Improving Critical Infrastructure Cybersecurity, Version 1, National Institute of Standards and Technology, February 12, 2014.
5. Mobile Technology Fact Sheet, Pew Research Internet Project, available at http://www.pewinternet.org/fact-sheets/.
6. Franklin Morris, "SMB Cloud Adoption Trends in 2014," *PC World*, October 7, 2014.
7. "Who's in the cloud?," Cloud computing in state and local government, Microsoft Government.

ROB ROQUE is technology services manager in the GFOA's Research and Consulting Center in Chicago, Illinois.