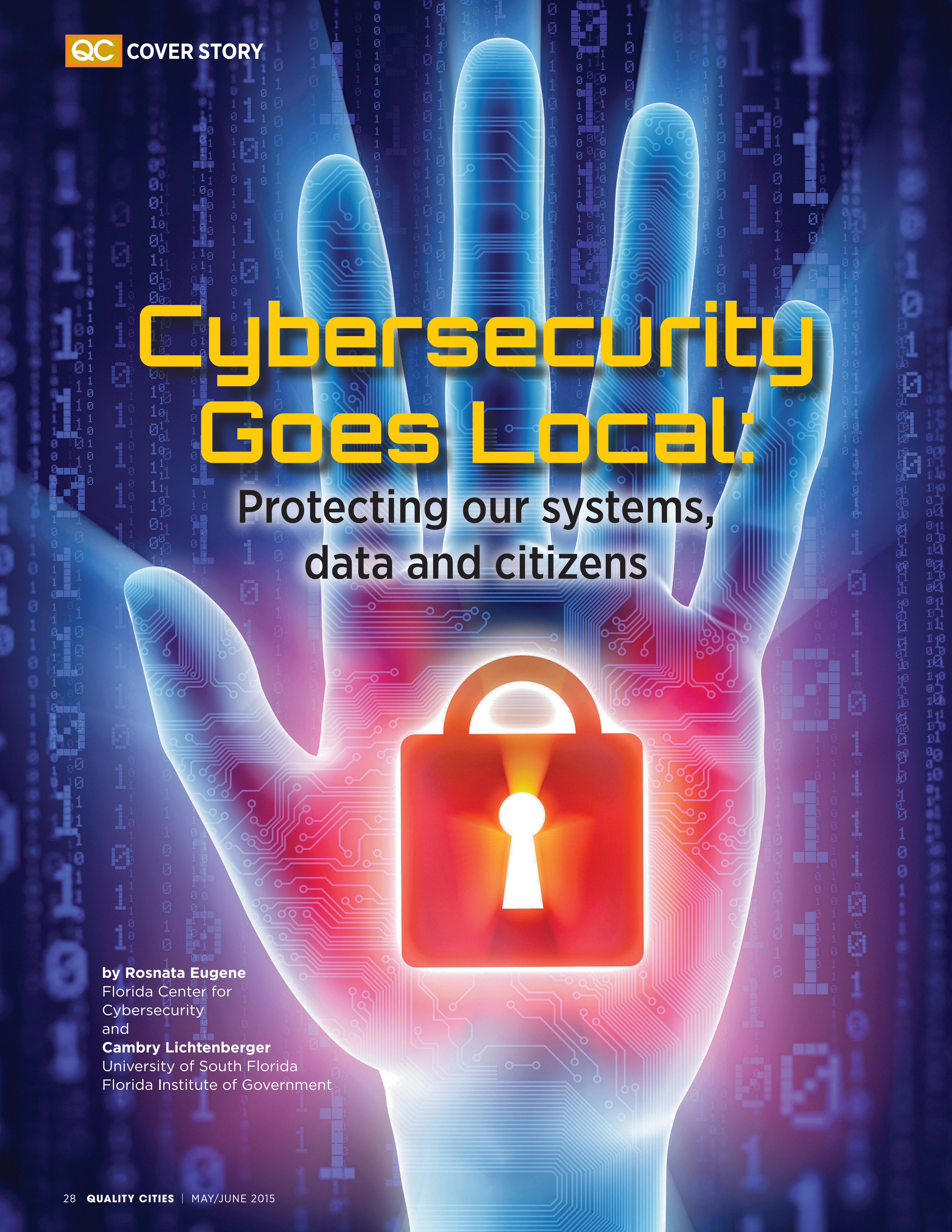

Cybersecurity Goes Local:

Protecting our systems, data and citizens

by Rosnata Eugene
Florida Center for Cybersecurity
and
Cambry Lichtenberger
University of South Florida
Florida Institute of Government

Officials from the **City of Wichita, Kan.,** must have found themselves thinking that, indeed, there is "no place like home" when the city's systems were attacked in 2013.

Wichita's city e-procurement website unknowingly caught the eye of **TurkishAjan,** a Turkish hacker group that successfully gained unauthorized access, stealing social security numbers, taxpayer information and banking data.

This sophisticated hacking operation affected more than 29,000 accounts, including local vendors with direct deposit business accounts, residents and 16 years' worth of employee expense reimbursement records.

"It was clear that they were not in Kansas anymore," according to **Cheri Lampel,** data security analyst with the **Florida Center for Cybersecurity (FC²).** "They were in the land of cyberwar."

WICHITA IS NOT ALONE

Attacks on government systems, like what happened in Wichita, show why cybersecurity has become a hot topic in public policy, and underscores the need to develop processes that address and counter cybercrime.

Although most of the conversations concerning cybersecurity focus on federal approaches, any level of government is susceptible to the risk and threat of cyber attacks. To put this problem in perspective, a 2014 global economic crime survey found that 7 percent of American organizations lost upward of $1 million or more due to cybercrime incidents in 2013.

Some local governments have learned the hard way just how dangerous hackers can be and how they can exploit systems.

Attacks on personal and financial records similar to Wichita are common, but they are not the only target. City infrastructure was up for grabs in **Springfield, Ill.,** when a pump at a public water facility was compromised and destroyed by someone using an I.P. address based in Russia.

These incidents demonstrate why cybersecurity matters to local governments and thankfully, there are proactive measures that identify and address cybersecurity gaps.

THE IMPORTANCE OF A PLAN

Governments at all levels face a multitude of challenges related to cybersecurity, such as insufficient funding, sophisticated threats and rapidly changing technology.

Officials and community stakeholders have voiced their biggest obstacles to comprehensive security: a lack of awareness and policy, and a lack of recovery plans.

Local governments can start developing their own policy by conducting a formal risk assessment, which can be done by organizations of any size.

The basis of the assessment starts with determining what information needs to be protected. Comparing these outcomes to systems already in place is where cybersecurity gaps are discovered.

Addressing these gaps takes the form of a cybersecurity plan: actionable steps that secure computers, networks, email and other tools.

The cybersecurity plan includes:

- how assignments are delegated;
- who is monitoring devices;
- how devices are being protected;
- if devices are being updated and, if so, how often;
- an adopted framework to guide the security management team such as the National Institute of Standards and Technology (NIST); and
- which activities or processes could pose a threat and how to address the threat.

An accompanying recovery plan applies these goals and objectives to an operating procedure for when systems are attacked.

Lampel states that "one of the key steps in preparation is developing an approach that is collaborative and dynamic." Crucial to a successful plan is engaging officials and technical/security staff to examine the plan together to ensure the objectives are attainable and in the best interest of the organization.

Like all sectors, governments are balancing the need for security against the need for usability and the implementation of new technologies.

New Technology . . . Increased Threat

While technological changes may enhance overall usability, they each bring added cybersecurity concerns.

THE CLOUD

Cloud storage, in which documents and data are stored remotely, allows workers to access their files and share information from any location. But without proper cybersecurity controls there may be associated risk, allowing hackers to compromise the security of files and information.

"In its infancy, cloud security was pretty shaky and not trusted by most organizations for production use," explained **Mike van Zwieten,** director of technology services for the Florida League of Cities. "But security has gotten much stronger, and it keeps improving to the point where many large organizations, governments, and even law enforcement agencies, which have challenging Criminal Justice Information Systems requirements, are starting to utilize cloud services."

He stresses the need for appropriate controls and protections, such as encryption and assurances that the cloud provider has the appropriate defenses in place and abides by industry compliance standards. Reputable cloud providers employ security staff and implement tools that tend to be state of the art and that, oftentimes, local governments can't afford.

LEFT: PHOTO©ISTOCKPHOTO.COM

However, information security also falls back on to the organization. "The city's technology staff will serve as contract managers ensuring there is a strong service-level agreement that protects the city and guarantees there are safeguards in place to keep data safe and secure," van Zwieten said.

> **Governments at all levels face a multitude of challenges related to cybersecurity, such as insufficient funding, sophisticated threats and rapidly changing technology.**

BRING YOUR OWN DEVICE

Another way that governments, along with businesses, have enhanced usability is to allow workers to use personal electronic devices, such as laptops, cell phones and tablets, for work.

Enhanced productivity as a result of **"Bring Your Own Device" (BYOD)** policies are coupled with the chance of software exploitation or other vulnerabilities of these devices.

Personal devices connected to work computers can be transformed into a remote keyboard, allowing hackers to control the computer. They could also manipulate that device's microphone and camera in order to steal files on the network.

Clicking unknown links, unknown linked images and files, or using devices without updated security patches are just a few examples of how hackers can most easily compromise an organization by exploiting BYOD.

Being mindful of these types of suspicious content encountered on personal devices is the first step in secure BYOD practice. Having devices connected to a virtual private network (VPN) and limiting access to files when not connected are means to block outside sources from taking advantage of personal devices and network systems.

SOCIAL MEDIA

Social media, like BYOD, is a popular trend in government that also comes with potential cybersecurity risk. Governments often use multiple platforms that serve to collaborate internally or engage with citizens.

Social media has proven so reliable that it is being integrated into statewide incident response and emergency management plans.

A primary communication channel during Hurricane Sandy, social media was where government agencies and citizens communicated directly and immediately throughout the disaster. This direct interaction with citizens has become incredibly valuable as a result of these events, becoming a necessary tool for governments to communicate.

With these advantages come potential threats: a breached account could disseminate false information or be used as a stepping stone into the organization's system. Close monitoring of these platforms can help prevent security threats.

Current trends like these are continually being incorporated into governments' every day practice. By establishing guidelines as part of the cybersecurity plan, organizations can address potential cybersecurity gaps and concerns.

There's a need for the precaution. Forty percent of governments report a sharp increase over the past few years in the number of cyber incidents associated with malware.

SAFETY PRACTICES

Common vulnerabilities can be tackled by implementing antivirus and firewalls, which protect systems from incoming

Promoting Cybersecurity Throughout Florida

To position Florida as a national leader in cybersecurity, the **Florida Center for Cybersecurity (FC^2)** promotes cutting-edge cybersecurity research, interdisciplinary and collaborative education, and outreach to engage diverse stakeholder groups.

Established in 2014, the center is housed at the University of South Florida. In addition to promoting the cybersecurity efforts across Florida's 12 state universities, the FC^2 has been increasing cyber awareness in the community by hosting conferences, developing partnerships, creating training programs and helping organizations leverage resources.

The Florida Center for Cybersecurity has partnered with the **John Scott Dailey Florida Institute of Government** at the University of South Florida (USF FIOG) to engage state and local government agencies in an effort to promote cybersecurity awareness and training.

For more information about the FC^2, visit *www.thefc2.org,* and about the USF FIOG, visit *fiog.usf.edu*.

PHOTO©ISTOCKPHOTO.COM

FC² Cybersecurity Tips

Becoming cyber secure can be done in stages. While inclusive plans take time, some steps that can easily be implemented include:

1. Install software updates so that attackers cannot take advantage of known problems or vulnerabilities.
2. Lock your computers or any devices if you walk away as someone can easily walk up behind you and load malicious software onto your computer.
3. If you find a USB drive, do not plug it into your computer to view the content or to try to identify the owner (it could contain a virus!).
4. Make periodic backups of your information so that you have clean, complete copies.
5. When picking a password, use a combination of uppercase and lowercase letters, numbers and special characters.

threats, as well as encryption software that codes files themselves to be unintelligible without a secret key or password. Threat-tracking services delve deeper by focusing in on what hackers are actively targeting and subsequently eliminating threats and complex malware.

Protecting systems using cybersecurity controls is as important as understanding cybersecurity risks. Often, these risks are not easily identifiable. Crucial threats can range from simple human error to disgruntled employees who purposely sabotage an organization by stealing data or equipment.

Changing user permissions after employee leaves the organization and educating the staff and administration on cyber risks are methods to avoid common threats.

What makes the cybersecurity plan actionable is how the organization plans to address cybersecurity gaps using policy and a recovery plan.

To prioritize policy, governments can:

- establish a cybersecurity governance team by identifying stakeholders and tasking technical and security staff with administering the cybersecurity plan;
- potentially develop public-private relationships with local IT businesses if the need is greater than resources available;
- enforce policies, procedures and oversight processes; and
- define and handle risks associated with vendors (e.g. possible risks associated with cloud service providers).

Being prepared for an attack is just as important as working within the cybersecurity procedures. Operating as if your organization has already been or will be the target of a cyber-attack is one of the best ways to minimize damage.

RECOVERING FROM AN ATTACK

Having a recovery plan can allow an organization to detect intrusions early on, isolate the threats and respond more quickly in order to allow the organization to resume its daily activities.

A practical recovery plan should include the following information:

- a communication strategy to communicate internally and to the public if systems do come under attack;
- legal procedures for handling the attack and the aftermath;
- a prioritized list of critical systems within the organization;
- documentation of current computer data backup methods and frequencies;
- a recovery task list; and
- an evaluation period during which the plan is tested. This is perhaps the most important part, as it addresses potential problems not initially addressed.

Periodic review of the recovery plan is also important, as needs may change over time. Continually adopting enhanced processes and technology is a way to combat having outdated systems to counter sophisticated attacks.

TAKING CHARGE

So how can a proactive approach to cybersecurity be initiated to protect a city, its data and the citizens within that community?

Organizations can start making effective changes by:

1. Working with upper level management to clarify employee roles and responsibilities.
2. Having a security plan in place in the event of an unauthorized breach.
3. Developing administrative and employee access controls.
4. Monitoring devices by routinely performing security and software updates.

Being proactive and using preventative measures allows governments to protect not only their system security but the information and trust of vendors, businesses and the citizens served.

Rosnata Eugene is a graduate assistant at the Florida Center for Cybersecurity and Cambry Lichtenberger is an assistant with the Florida Institute of Government at the University of South Florida. QC

PHOTO©ISTOCKPHOTO.COM

The following two municipal technology experts were asked:

WHAT STEPS HAS YOUR CITY TAKEN TO IMPROVE ITS CYBERSECURITY EFFORTS?

KENT HAINES

IS Supervisor

City of Jacksonville Beach (population 22,136)

To enhance Jacksonville Beach's cybersecurity footprint, we installed the Cisco Adaptive Security Appliance firewall system. The Cisco firewall is a robust security system, allowing intrusion detection and prevention at the outermost ring of our perimeter.

Along with that, to prevent the entry of malicious email and files, we installed two devices from Bloxx – an email filtering device and an Internet filtering device. The Bloxx email filter allows users to report a specific email as spam, and the device "learns" the types of emails that are valid and extrapolates those that should be blocked. The new Bloxx email filter is currently preventing 87 percent of the emails from even reaching our email server, allowing it to operate more efficiently.

We have coupled this defense-in-depth methodology with a more robust user-training program. Now all users are required to attend a computer security seminar every year, hosted by the Information Systems Division.

MIKE ANDREWS

Network Manager

City of Leesburg (population 21,163)

Like most organizations, Leesburg doesn't have the luxury of limitless budgets or the time required to implement perfect security protection. But we all have the ability and responsibility to provide the highest possible level of security equipment, solutions, training, procedures and policies to mitigate risk and immediately respond to incidents.

In Leesburg, we spread our resources as evenly as possible, detecting and preventing intrusions with hardware security devices at the edge of the network, with endpoint security management systems, and with heuristic detection and behavior filtering on all traffic to and from any public networks.

We use centralized management and reporting solutions for operating system and application updates, and review any failures, exceptions or other anomalies. With subscriptions to numerous security notification systems, including MS-ISAC, Infragard and US-CERT, we have increased our awareness and preparedness. Some of this information is compiled and distributed as security best practices to users, educating them about threats like phishing emails, targeted social engineering and "drive by" and "watering hole" exploits, and training them on proper response and notification.