King County
Information
TECHNOLOGY

KING COUNTY CYBER SECURITY

Briefing for King County Council Committee of the Whole

September 21, 2016

Bill Kehoe – King County Chief Information Officer

King County
Information
TECHNOLOGY

What is cybersecurity?

- Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorized access.
- In King County this responsibility is addressed by KCIT Information Assurance group in collaboration with independently elected agencies.

What threats is the county facing?

The threats that King County faces are the same threats that all organizations face to differing degrees. We face the usual environmental threats such as fire, earthquake, flood, etc. As for Human threats the FBI has identified common types of "threat actors". Notable are:

- **Hactivists** – Hactivists use computer network exploitation to advance political or social causes.
- **Criminals** – These individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.
- **Insiders** – Trusted insiders steal proprietary information for personal, financial and ideological reasons. Trusted insiders are prone to error and mistakes. These individuals abuse their legitimate access within the organizations systems.

Cybersecurity is not a threat management issue; it is one of managing risk. This is because we cannot control the threats but we have some ability to manage and reduce the risks.

Risks related to cybersecurity can be categorized in three general areas:

- Unauthorized access to systems (confidentiality)
- Unauthorized data modification (integrity)
- System downtime / business interruption (availability)

We manage the risks not just through technology but also through people and process by managing vulnerabilities. A vulnerability is a weakness in a system or process that can be found in all organizations. The trick is to find them and fix them before an unauthorized person use them to their benefit or malicious intents.

What are we doing to address them?

King County has a duty of care to protect information with which it is entrusted from unauthorized disclosure, modification and/or destruction.

King County is managing vulnerabilities by monitoring the risks, both human and environmental. These vulnerabilities may be within the technology, facilities, a process or lack of awareness or training in our employees. Once discovered we seek means of reducing the risks by addressing the vulnerability. For example, employee security awareness training is one of the most effective and low cost mean to manage the vulnerabilities.

The following are measures the County has taken that have contributed to managing vulnerabilities:

1) Through consolidation and realignment, KCIT has provided increased efficiencies and synergies in managing vulnerabilities. It provides the ability to modernize antiquated systems, standardize on platforms and modernize applications that have more advanced protection.
2) Following industry best practices, KCIT also increases operational disciplines (such as ITIL and a System Development Life Cycle) and trains staff on those disciplines.

3) Migration to the cloud whether through Software as a Service (SaaS) or Infrastructure (IaaS) has also improved cybersecurity by adding resilience to King County's information systems.
4) Working with operations teams within KCIT and independently elected agencies, the Information Assurance team is constantly looking for any gaps in King County's security infrastructure and developing plans to address the associated risks.

What can residents and employees do to protect the county/ themselves?

Awareness is the first step for both employees of King County residents. Knowing what your risks are and how the "bad guys" exploit them is paramount.

Other recommendations are:

- Use strong passwords, Passwords that are not just words that can be found in a dictionary,
- Lock your PC or Laptop when away from your desk and never leave it unattended in a public place.
- Learn the difference between Spam and Phishing and be able to identify Phishing.
- Use good Internet practices.
- Never give out personal information such as SSN or Credit Card information online unless you know EXACTLY who you are communicating with.

This is just the beginning, each of these and more are part of being aware of the risks and how they are exploited

What to do if an "incident" occurs.

First, do not panic.

For King County employees the second step is to call KCIT's Service Center 263-HELP. They are trained to assist employees in addressing computer incidents.

Follow the instructions of the Service Center representative. From there KCIT will assume resolution and address the issue. We have an established Incident Response Process which is highly effective in restoring impacted systems. This process is always under review to find even more effective ways to respond and recover.

Residents of King County, should report the incident to the Federal Bureau of Investigations through the Internet Crime Complaint Center (IC3) Web site at https://www.ic3.gov. This report will not likely result in an investigation but allows law enforcement to track trends and accumulate information and potential evidence for prosecution should a perpetrator be apprehended.

Their next move is dependent upon the type of incident. Their best step is to find help to stop the effects of the incident. This may be a service technician to remove malware or their ISP to better protect their internet connection.