DRAFT

Not for distribution or publication.
Story placement review only.

CYBERSECURITY
is everyone's job.

Human Resources

People matter in cybersecurity

Local government human resources involvement is essential

As Human Resource professionals, you have a role to ensure your training program enables a cyber-aware and secure culture. You are also responsible for evaluating and supporting staffing needs to address cyber-risks.

Here are three things you can do in your role to #BeCyberSmart.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Last updated June 2019

It might seem like cybersecurity doesn't have much to do with the Human Resources (HR) department of a local government, but you actually have a vital role to play to #BeCyberSmart. There are many considerations when it comes to cybersecurity, but here are three main themes that are important for an HR professional to know. To start, you have an important role to ensure your training program enables a cyber-aware and secure culture. You are also responsible for evaluating and supporting staffing needs to address cyber-risks. You also maintain sensitive personnel information, such as home addresses, social security numbers, and even bank accounts. This data needs to be protected against unauthorized access, which is an important part of cybersecurity for an organization.

1 Train employees on cybersecurity

Your vital role in HR includes responsibility for staff training of all kinds—make sure the staff in your local government organization have access to cybersecurity training. Governments need to have a cybersecurity awareness and training program for all employees that includes elected officials and employees. Training should include information about the entity's policies related to cybersecurity and might also be awareness about various risks such as how to detect and report fraudulent emails or how to handle sensitive information. A local government's cybersecurity training program could be differentiated for various groups or departments based on risks unique to their roles.

Guidance to help build a training program from the Center for Internet Security

2 Evaluate and support staffing needs to address cyber-risks

HR plays an important role in staffing - including helping information technology make sure it has the staff to address cyber-risks. Retaining quality employees is equally as important; local governments could provide opportunities to learn new skills as well as include employees in decision-making and innovation

Department of Homeland Security issued a Cybersecurity Workforce Development toolkit. This includes information needed to help you build your cybersecurity workforce.

3 Protect access to sensitive employee information through cybersecurity best practices

Human Resource departments have highly confidential data (such as social security numbers, home addresses, phone numbers, bank accounts) used in recruiting, evaluating employee performance and providing compensation and benefits. In working together with your information technology department, you can make sure there are protections in place for your HR management system to prevent unauthorized access and service disruption. This might include strong passphrases and multi-factor authentication.

In addition, HR should work with the information technology and legal and compliance departments to ensure any vendors or other third parties with access to sensitive and confidential information comply with required policies, laws and regulations.

HR should work together with leadership to adopt policies defining sensitive and confidential information. These policies should identify how to protect and share the information. An example might be using encryption to transfer data to a third party.

For more information about multi-factor authentication: www.cisecurity.org

People matter, and HR plays a key role

A properly-trained staff can be your local government's most important protection against cyber-risks. Furthermore, an information technology department equipped with the security expertise it needs to address threats is key. HR is vital to ensuring all of these areas are addressed.

Our Office also offers training at conferences on cybersecurity. For upcoming dates and times - visit

sao.wa.gov/BeCyberSmart

Sources:

Department of Homeland Security
National Institute of Standards and Technology