CYBERSECURITY
is everyone's job.

Human Resources

People matter in cybersecurity

Local government human resources involvement is essential

As human resources 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

Updated October 2021

You might not realize it, but as a human resources (HR) professional, you have a vital role to play in cybersecurity. To start, you have an important role to ensure your training program enables a cyber-aware and -secure culture. You are 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, which must be protected against unauthorized access.

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, including elected officials and others.
Training should include information about the entity's policies related to cybersecurity and could also increase awareness about how to address various risks, such as detecting and reporting fraudulent emails or handling sensitive information.

A local government's cybersecurity training program could be differentiated for various groups or departments based on risks unique to their roles.

Here is a resource to consider:

Center for Internet Security guidance to help build a training program: https://www.cisecurity.org/blog/keep-your-employees-interested-in-cybersecurity-awareness-training-with-these-tips/

2 Evaluate and support staffing needs to address cyber risks

HR plays an important role in staffing — including helping to ensure the information technology department has the staff needed 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.

Here is a resource to consider:

Department of Homeland Security Cybersecurity Workforce Development toolkit: https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf

3 Protect access to sensitive employee information through cybersecurity best practices

Human resources 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.

Here is a resource to consider:

Multi-factor authentication information from Center for Internet Security: http://www.cisecurity.org/newsletter/securing-online-accounts-with-multi-factor-authentication/

People matter, and HR plays a key role

A properly-trained staff can be your local government's most important protection against cyber risks. Further, 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.

To learn more, visit

sao.wa.gov/BeCyberSmart

Sources:

Department of Homeland Security
National Institute of Standards and Technology
Center for Internet Security

Center for Government Innovation