THE MAGAZINE OF THE INTERNATIONAL PUBLIC MANAGEMENT ASSOCIATION FOR HUMAN RESOURCES

OCTOBER 2018

HR NEWS

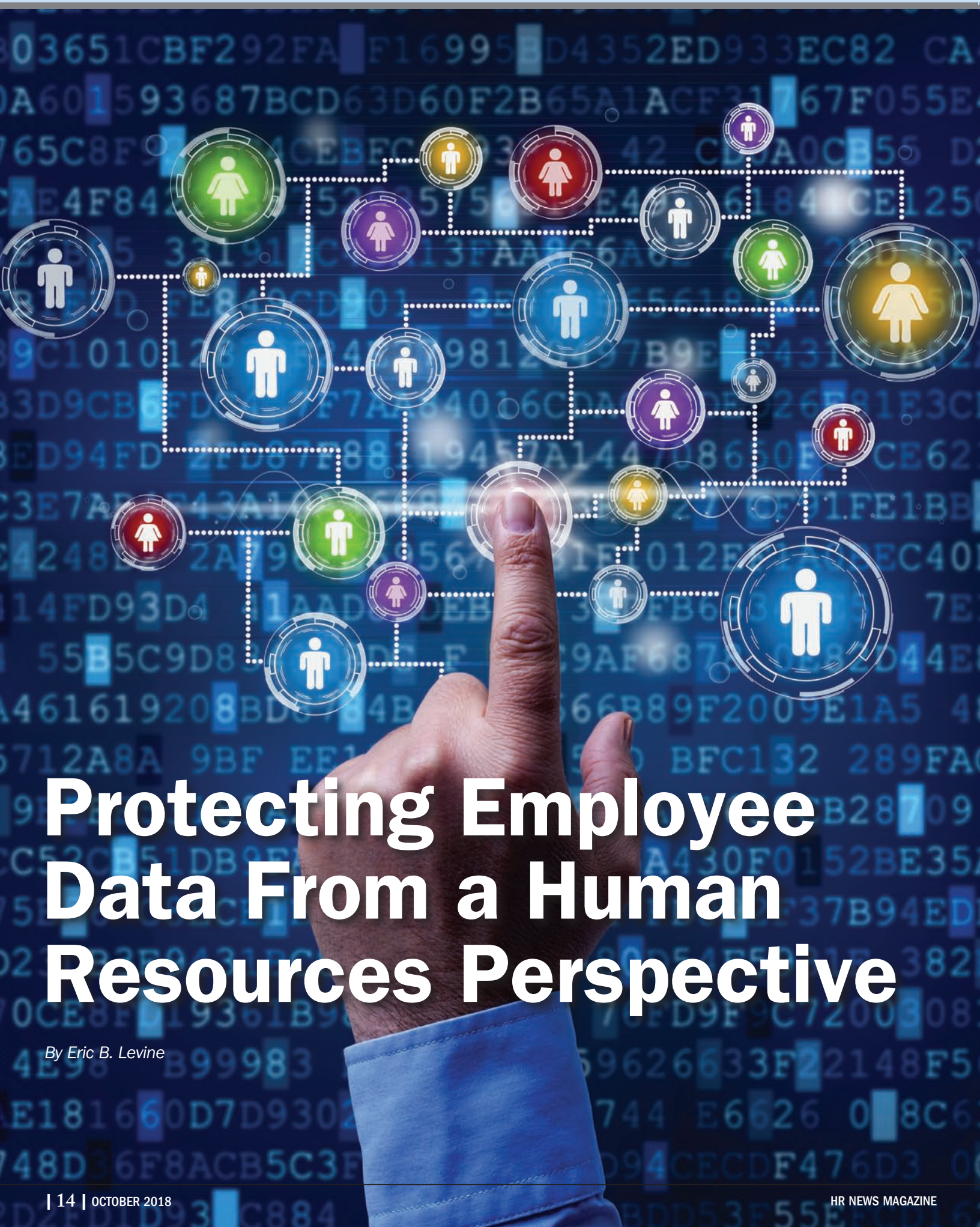
IPMA-HR

Communications and Social Media

Keep Conversations on Equality at Work Open and Productive

Emojis Run Amok?

5 Steps to Conduct an Effective Social Media Recruitment Campaign



Protecting Employee Data From a Human Resources Perspective

By Eric B. Levine

Combatting cyberthreats and protecting data is not just the job of IT specialists. Human resources professionals in the public sector must also safeguard personally identifiable information.

Every agency possesses a literal treasure trove of sensitive information about its employees, and the HR staff has access to it all. It is difficult to think who else could call up any other staff member's name, address, date of birth, Social Security number, bank account information for making direct deposits, health and medical information, and retirement plan information with no more than a few keystrokes.

Needless to say, a data breach implicating your department could be devastating. So what can you, as an HR professional, do to maintain the integrity of personally information? Plenty.

Collaborate With the IT and Legal Departments

In order to know how to protect employee data, you must first know what data you have and where the weaknesses in data maintenance are. HR department heads should meet with their IT counterparts to ensure they understand the various data privacy threats the agency and their own department face.

Similarly, meeting with your agency's counsel and discussing specific legal obligations regarding data privacy is helpful, as it allows the organization to take additional steps to ensure compliance. For example, HIPAA requires that individuals affected by a medical records data breach receive notification within a specific timeframe. Many states' data privacy laws do not impose a similar requirement.

While not needing to be an IT or legal expert, the head of HR should develop a solid understanding of how data is maintained and utilized. Doing this will help ensure that the agency has an adequate knowledge base for making decisions and taking protective or corrective actions.

Education and Monitoring

HR professionals must ensure that everyone who works in their organization takes part in training on topics such as securing mobile devices, safeguarding data while working remotely, creating and changing passwords, and recognizing common cyberthreats like social engineering, phishing and ransomware. Such training must be mandatory and updated every year or two. Further, attendance at or completion of training sessions should be documented in each employee's personnel file.

Setting such rules will ensure that employees' education is current and create a record of reasonable training should evidence be needed to defend the organization against litigation following a hack or data theft. Providing and documenting data protection training may also be a condition for holding a cyber insurance policy.

Beyond training, HR should consider monitoring employees' computer use to detect unauthorized information access or unusual download activity. It is essential, however, to put a computer privacy policy in place before doing any monitoring. That policy must include a requirement to advise employees that they will be monitored and should never expect anything they do using a work computer, tablet or smartphone to be private.

Giving such notice satisfies legal requirements. It can also deter some employees who would otherwise not limit their use of work computers to doing actual work. This, in turn, reduces the chances of employees accessing suspicious websites at work.

Every agency possesses a literal treasure trove of sensitive information about its employees, and the HR staff has access to it all.

Start doing data privacy training during the onboarding process by providing new hires with copies of all data privacy policies and by walking them through procedures. Encourage employees from their first day to understand that alerting managers of any possible data breaches in a timely manner is crucial. Also make sure that employees know that while all data privacy events must be reported, innocent mistakes happen. Do not hesitate to discipline bad actors for breaching data privacy protocols, but also strive to foster an environment in which employees feel free to report problems and do not fear retribution for being a bearer of bad tidings.

Finally, be vigilant and watch for employees who are dissatisfied with work and may be prone to going rogue and destroying materials or taking sensitive materials with them when quit or get fired. In the worst case scenario, an angry employee may try to harm your organization by releasing sensitive information. One way to prevent employees from doing things like that is to encourage them to share their grievances with your HR office so that problems can be discussed and, hopefully, resolved.

Eric B. Levine is a partner with Westfield, N.J.-based Lindabury, McCormick, Estabrook & Cooper, P.C., and co-chair of his firm's Cybersecurity and Data Privacy practice. You can contact Levine via email at elevine@lindabury.com. –N