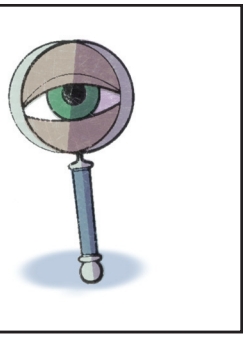
PHILLIPS LYTLE LLP ALERT
FOR BNHRA MEMBERS
DATA SECURITY & PRIVACY
JULY 2017



Managing the Human Element of Cybersecurity: an Employee Lifecycle Control Structure

Cybersecurity threats are not limited to only cyberspace; a human component exists that must be mitigated. What division of a firm's organization understands its employees better than Human Resources ("HR")?

HR has the skills necessary to detect and control two potential insider threats to an organization's cybersecurity. First, the well-intentioned employee who makes a mistake (e.g., sending confidential information to a personal email address rather than a work-related email address). Second, a disgruntled employee who has ill will towards the organization (e.g., a former employee who was recently fired and seeks retaliation).

Employees need to be acutely aware of the organization's cybersecurity policies and procedures, trained in the proper application of the policies and procedures, and understand (and accept) their personal responsibilities and accountabilities. This alert provides an employee lifecycle control structure that HR professionals can implement to improve cybersecurity within their organization.

1. NEW EMPLOYEE — ONBOARDING

New employees bring more than their skills and experience to the workplace – many also bring poor cybersecurity habits. To minimize the risks being brought by new employees, it's essential that HR incorporates cybersecurity into the onboarding process.

Screening Confidential Information

New employees should understand that use of sensitive data from their prior employer(s) is not condoned in the employee's new organization. This message should be clearly communicated even before the employee's first day on the new job.

Training and Attestation

A cybersecurity training should be administered as soon as a new employee joins the organization. All of the organization's policies and procedures relating to cybersecurity should be provided to the new employee. An attestation, stating training and documentation review has been completed and the new employee understands his or her responsibilities, should be signed by the new employee and submitted to HR for recordkeeping.

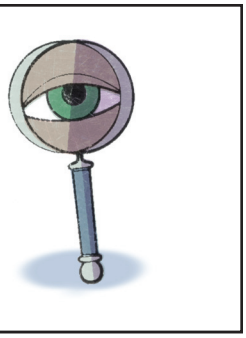
2. CURRENT EMPLOYEE — DEVELOPMENT

Current employees have the greatest access to an organization's systems and information. As such, a control framework should be implemented, monitored and updated to mitigate the constantly changing cybersecurity risks impacting an organization.

Policies and Procedures

Organizational policies and procedures relating to cybersecurity should be documented in sufficient detail to serve as a reference for employees in their day-to-day activities. At a minimum, HR should seek to address:

- Privacy. Employees should have no expectation of privacy in the organization's electronic systems, which may be monitored for the organization's data security purposes.



- Remote Mobility. Corporate systems and information accessed through an employee's personal devices are confidential and subject to the same standards as if the employee was using his or her office computer. For example, employees should refrain from taking screenshots of corporate information using their personal cell phone or printing corporate documents on their home printer, which may maintain an electronic version of the document on the printer device.
- Clean Desk Protocol. Sensitive information in hardcopy or electronic form should be secure before an employee leaves their workspace, irrespective of the amount of time they plan to be away. For example, if an employee leaves their desk to retrieve a document from the printer, the employee should lock and password-protect their computer if sensitive information could be viewed by an unauthorized person.
- Social Media. Define appropriate social media uses and include and identify some of the risks employees should consider before creating online content, even in their personal use. Confidential proprietary information should not be disclosed in personal social media posts. In certain industries (e.g., financial services), social media communications may be considered prohibited advertisements or solicitations, resulting in potential civil or criminal penalties, including suspension of professional licenses.
- Incident Response. In the event of a data breach or a cyberattack, a detailed procedure should be in place for employees to follow.

Training

Employees should receive specific and comprehensive periodic training that reinforces and helps implement written policies and procedures. Training should ideally be conducted by a third-party subject matter expert.

Monitoring and Surveillance

Periodic review of employee electronic communications is an organized and risk-focused way to identify procedural or training weaknesses within an organization. Findings should be escalated to management to resolve deficiencies, if appropriate.

Performance Evaluations

Data security responsibilities should be built into an employee's role description and their personal objectives to encourage accountability.

3. DEPARTING EMPLOYEE — OFFBOARDING

Those who pose insider threats typically conduct their illicit activity near the time of announcing their resignation. Similarly, a hasty termination may pose additional risks.

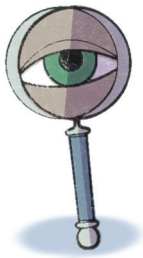
- Disablement Procedure. Upon immediate notice of resignation or termination, an employee should have limited to no access to the organization's systems. HR should partner with the Information Technology division to ensure this objective is consistently achieved.
- Monitoring and Surveillance. A 30-day electronic communications review, with special consideration given to emails containing attachments, should be conducted after an employee has left an organization. This review should be publicly communicated to employees to deter prohibited behavior. Findings should be escalated to management to resolve deficiencies, if appropriate.

PHILLIPS LYTLE LLP ALERT

FOR BNHRA MEMBERS

DATA SECURITY & PRIVACY

JULY 2017



Practical Matters

The multidisciplinary Data Security & Privacy Practice Team at Phillips Lytle engages the expertise of attorneys with important and necessary perspectives on a variety of areas. Our attorneys are former technology business owners, labor and employment executives, and those with in-depth HR industry experience, making us uniquely qualified to evaluate and develop policies and procedures, as well as deliver targeted trainings specifically tailored to the ever- evolving cybersecurity risks facing organizations.

Additional Assistance

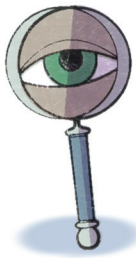
For questions regarding data security and privacy matters, please contact Jennifer A. Beckage at (716) 847-7093, jbeckage@phillipslytle.com, or any of the attorneys on our Data Security & Privacy Practice Team. ■

PHILLIPS LYTLE LLP ALERT

FOR BNHRA MEMBERS

DATA SECURITY & PRIVACY

JULY 2017



Data Security & Privacy Attorneys

Jennifer A. Beckage (716) 847-7093, (212) 759-4888 ext. 7093, (585) 238-2000 ext. 7093 jbeckage@phillipslytle.com
Edward S. Bloomberg (716) 847-7096, (212) 759-4888 ext. 7096 ebloomberg@phillipslytle.com
Alan J. Bozer (716) 504-5700, (212) 759-4888 ext. 5700 abozer@phillipslytle.com
Mary E. Burgess (518) 472-1224 ext. 1231 mburgess@phillipslytle.com
Anna Mercado Clark (212) 508-0466 aclark@phillipslytle.com
Jeffrey D. Coren (716) 847-7024 jcoren@phillipslytle.com
John M. Falk (202) 617-2723 jfalk@phillipslytle.com
Chad W. Flansburg (585) 238-2009 cflansburg@phillipslytle.com
F. Kenneth Graham (716) 847-7049 fkgraham@phillipslytle.com
Asaf Hahami (212) 508-0432 ahahami@phillipslytle.com
Patrick M. Hanley, Jr. (716) 847- 8306 phanleyjr@phillipslytle.com
Luke B. Kalamas (585) 238-2035 lkalamas@phillipslytle.com
Timothy P. Kucinski (716) 847-7056 tkucinski@phillipslytle.com
Brendan S. Lillis (716) 847-7058 blillis@phillipslytle.com
Richard J. Marinaccio (716) 504-5760 rmarinaccio@phillipslytle.com
Mark J. Moretti (585) 238-2004, (212) 508-0404 mmoretti@phillipslytle.com
William V. Rossi (716) 847-7022 wrossi@phillipslytle.com
John G. Schmidt Jr. (716) 847-7095, (212) 508-0426 jschmidt@phillipslytle.com
Gargi Sen (716) 847-7051 gsen@phillipslytle.com
James Kevin Wholey (202) 617-2714 jwholey@phillipslytle.com

Phillips Lytle LLP

Albany Omni Plaza 30 South Pearl Street Albany, NY 12207-3425 (518) 472-1224
Buffalo One Canalside 125 Main Street Buffalo, NY 14203-2887 (716) 847-8400
Chautauqua 201 West Third Street Suite 205 Jamestown, NY 14701-4907 (716) 664-3906
Garden City 1205 Franklin Avenue Plaza Suite 390 Garden City, NY 11530-1629 (516) 742-5201
New York City 340 Madison Ave 17th Floor New York, NY 10173-1922 (212) 759-4888
Rochester 28 East Main Street Suite 1400 Rochester, NY 14614-1935 (585) 238-2000
Washington, DC 800 17th Street NW Suite 450 Washington, DC 20006-3962 (202) 617-2700
Canada The Communitech Hub 151 Charles Street West Suite 152 The Tannery Kitchener, Ontario N2G 1H6 Canada (519) 570-4800