2016 HOSPITALITY LAW CONFERENCE

ROUNDTABLE: EMPLOYEES ARE A SOFT SPOT IN DATA SECURITY

Data thieves can penetrate your company's electronic systems in a large variety of ways. But where are the weakest points in your security? One place where weaknesses are likely to exist is in your own employees, through their lack of security awareness and dangerous habits. In fact, a number of industry security experts have identified a company's employees as its most vulnerable point from a data security perspective.

What can companies do to reduce the likelihood that the actions or inactions of their employees will lead to a compromise in data security? Here are some suggestions:

1. Take your employees out of the equation as must as possible. It is difficult to try to teach employees to be secure, and many experts are saying that training produces mixed results at best. Companies should focus on securing the environment and segmenting their computer networks. If it's safe for your employees to click on any link, open any attachment, without risk of harming the organization, then you've short-circuited the possibility of an inattentive employee clicking on a link and allowing cyber thieves into your system.
2. Limit which employees have access to sensitive data.

   Not all data is created equal. Much of the data maintained by most companies is not sensitive and/or does not include personally identifying information ("PII"). However, all companies have employee data, many have personal customer data, and many have trade secret or business confidential information.

   There is typically no need for everyone in your organization to have access to everything maintained in your systems. The smaller the number of employees who can access

stored customer and employee PII, or trade secret material, the less chance that a system will be exposed through employee actions or inactions. Therefore, employers should make judgments about which employees must have access to which data, and should err on the side of giving less people access where it is not truly needed.

3. Control password creation and train employees on password strength and security.

   A significant number of system breaches result from the intruder's acquisition and unauthorized use of login credentials of company employees. In many instances passwords are compromised because: (1) they are allowed to remain unchanged for overly long periods of time; (2) the employee discloses his password or leaves it written on a sticky not on his monitor; or (3) the employee chooses a password that is weak and easily guessed, especially when the cyber intruder is using software to help with that guess.

   Have your IT department take control of password security by: (a) requiring passwords to be changed regularly; (b) requiring a sufficiently complex combination of characters, letters and numbers to make the password strong and difficult to guess; and (c) enforce policies prohibiting communication of passwords to others.

4. Train employees to be careful of phishing.

   Many significant breach incidents have begun with an employee getting an e-mail that he believes to be legitimate or harmless, and clicking on a link or attachment in that e-mail. Phishing has become more and more sophisticated. Perpetrators of phishing scams have gotten better at disguising e-mails with real-looking company logos and personal information about the recipient, thus creating a sense that the e-mail is legitimate and can be trusted.

Security companies have developed training programs to strengthen employee awareness and care surrounding phishing e-mails. They teach employees to recognize suspicious indicators, then send "test" phishing e-mails to determine whether employees are applying what they learned, and whether additional training is required.

5. Create and enforce policies limiting internet access and prohibiting unauthorized software.

   Employees can inadvertently introduce malware into your systems acquired from internet websites they have visited or from suspect software programs that the employee accesses or loads onto his work computer. While your company's anti-virus software may screen out many such threats, some malware can circumvent those protections. Keeping out malware from these sources by training your employees not to engage in risky behavior is the first line of defense against attacks mounted from such sources.

6. Police and train employees in the use of mobile devices.

   Laptops, tablets, smart phones, flash drives – all of these are regularly used by employees to transport or access company data from outside of the workplace. Data thieves have developed sophisticated methods of attacking mobile devices through, for example, false Wi-Fi networks. However, at times the mobile devices themselves are simply lost or stolen. Employers can cut down on the security dangers presented by mobile devices by: (1) controlling what data may be stored or accessed remotely by employees; (2) encrypting information stored on mobile devices; and (3) training employees on the safe usage of mobile technology.

7. Create a culture of security awareness and a sense of shared responsibility.

   Security awareness comes from the top down. If decision makers and upper level management show that they are very serious about data security, employees will take note and treat it seriously as well. Things that help to achieve this shared sense of responsibility are: (1) create and update data security policies, and teach them to your employees; (2) use mandatory training on security issues and practices; and, (3) recognize and reward good security practices.