

This story appeared on CSO Online at
<http://www.csoonline.com/article/print/343968>
5/6/08

Five Ways to Turn Employees into Security Assets for Protecting Data

Trend Micro's Glen Kosaka explains how to prevent data leaks by raising security awareness and gaining employee support
Glen Kosaka, director of DLP products, Trend Micro

Never before has the threat to corporate data assets been so great—and so costly. According to Attrition.org, an industry monitoring organization, in 2007, more than 162 million records such as credit cards and social security numbers were compromised through December 21—both in the U.S. and overseas. The Identity Theft Resource Center lists more than 79 million records compromised in the U.S. through December 18, 2007. That's nearly a fourfold increase from the 20 million records reported as compromised in 2006.

The explosion of messaging systems, wireless networking, and USB storage devices has made the protection of critical enterprise data even more difficult than it was before. Increasingly, enterprises are operating as "borderless" organizations, sharing information globally between employees and partners. These borderless enterprises are challenged to balance openness and flexibility with security and risk as employees work from home or in coffee shops and other off-site locations when they travel. However, most breaches and loss of sensitive data are caused by employees who are uneducated and therefore inadvertently put their company at risk. Because most breaches are accidental, companies have an opportunity to better protect enterprise data by educating employees on the proper handling of information.

Here are five ways to turn employees into security assets instead of liabilities:

Make data security part of the company culture

Protecting sensitive information should not be the sole responsibility of the security and executive teams. Every department manager has the responsibility to help identify and locate sensitive data, and to propose policies for the appropriate access, use, and protection of that data by employees. Each employee who has been identified as having access to sensitive data should undergo training on the policies and procedures which define responsible care for the company's data. In this way employees and managers alike share the responsibility for not only their own use of sensitive data but also can serve to watch over others to ensure that everyone is observing these policies.

Integrate data leak prevention processes into overall workflow

Many companies have lost control over their sensitive data because the identification, access to, and movement of sensitive data is not integrated into their overall processes. For example, when new documents or content are created, is there a classification process to determine the appropriate policies which apply? Or when employees join a department or transfer between departments, are processes initiated for data protection and access controls for new and prior departments. In addition, the introduction of new mobile devices or remote development sites can introduce new threat vectors for data leaks. When companies think through their core processes, and incorporate data protection steps as appropriate, the risk of data leaks is reduced significantly.

Make employees feel like security assets, not liabilities

If employees can feel as vigilant about protecting their company data as they do about meeting other business objectives, they become an extremely valuable asset to their company's data security programs. Saving their company from millions of dollars in fines and expenses associated with a breach can be as valuable as saving the company millions from improved

processes or reduced costs, not to mention the embarrassment and loss of goodwill associated with privacy breaches. Training and awareness programs around the costs of various types of breaches and what they can do to prevent breaches will sensitize employees to the challenges faced.

Prevent the temptation to engage in "harmless" policy violations

While there are many obvious "no-no's" such as selling the company account list to a competitor, there are many "grey area" violations which, if left unaddressed, can lead to more damaging breaches. These include sharing contact lists with friends at other companies, "backing-up" sensitive data to home systems or unauthorized storage devices, and copying intellectual property to USB thumb drives to transport them to a remote development site. All of these violations, while they may seem harmless to the employees who commit them, can lead to costly breaches. In addition, as employees are allowed to push the envelope of what they can get away with, there may be increased temptation to profit from these violations. While there are many alternatives for monitoring and enforcing policies, the selection criteria of a data leak prevention (DLP) solution should include the intelligence of the solution to detect relevant leaks without inconveniencing the employee and impacting their business (and, for some companies, personal) productivity.

Teach employees about policies while enforcing them

An effective data security policy should incorporate a "carrot and a stick" approach. Employees should be educated about the company policies, ideally at the "point of use" or "point of violation." When an employee copies a sensitive document to a USB drive in violation of policy—that is the best time to educate them about the proper protection of the company's valuable assets. If violations are severe, the action should be blocked by the DLP solution, and the employee's management should be notified so proper steps can be taken. Raising employee awareness of data protection policies, especially at the "point of use," can reduce or even eliminate the large percentage of breaches which occur accidentally and unintentionally.

Data leak prevention technology should not only monitor and prevent leaks, but help to educate and raise the awareness of employees about company policies and procedures for handling sensitive data. By educating employees and safeguarding both the network perimeter and internal endpoints, DLP solutions also can help employees become security assets by preventing data leaks, reducing accidental breaches and requiring their vigilance to protect sensitive data.

However, any new technology that affects the daily activities of employees must be intelligent and accurate to avoid reducing employee productivity and creating frustration. A fine line must be drawn between monitoring and enforcing critical data leak prevention policies and enabling employees and administrators to do their jobs and keep the business growing.

Glen Kosaka is the director of DLP products for Trend Micro
© CXO Media Inc.