BTB SECURITY

WHEN SECURITY IS AN INSIDE JOB

IN MANY COMPANIES, IT AND HR DON'T HAVE MUCH IN COMMON.

After all, one is in charge of the technology while the other is in charge of the people. But this can create a dangerous gap in communications, one that can lead to a potentially devastating data breach or theft of intellectual property.

In CA Technologies 2018 Insider Threat report, 90 percent of organizations reported they felt vulnerable to insider attacks while only 6 percent said they were not vulnerable at all. In addition, a majority (53 percent) of respondents confirmed that insider attacks were initiated against their organization during the previous year. And, finally, 27 percent of responding organizations indicated that insider attacks have become more frequent.

These attacks can occur before, during or after an employee leaves the organization. An employee who's received a bad performance review and is on probation may seek revenge. A high-level employee may have given their two-week notice – perhaps to join a competitor – and uses the time to download sensitive company information. Or a former employee may have installed a backdoor so they can still get into the company's network.

In all of these cases, IT may not have known that the employees were on their way out or had already left. And, even if they did, IT may not have standard practices in place to guard against the damage these employees could do. That's why it's so important to create a communications channel between HR and IT. HR needn't divulge sensitive details about the employee. What it does need to do is make sure to alert IT to monitor or shut down specific accounts.

If an employee is on probation or has resigned, IT should be watching their online activity. Disgruntled employees have been known to download files of sensitive company data like client lists, emailing them to their home or to a private Dropbox account or, worse, to a competitor. If the employee is fired, all access should be closed down while HR is informing them. Unfortunately, it's common for companies to allow employees to return to their desks before informing IT of their change in status. Sometimes, IT never knows the employee left, which leads to an accumulation of "ghost accounts" on your network.

Other times, they know but are in no rush to shut off access. This is when really bad things can happen.

"Privilege creep" is also common as start-ups or small companies grow. In the CA Technologies report, excessive access privileges was rated as one of the top risk factors in a company's vulnerability to insider attacks. In the early days, it's often "all-hands-on-deck" and there may not be an IT department, so employees are given total access to allow them to do whatever needs to be done. In some instances, an employee is given access to a particular capability while working on a special project. This can become a problem if these privileges are never reassessed or removed.

IT employees are of special concern because they know the ins and outs of your systems. For example, say your senior IT person has just announced their resignation. How do you know they haven't already stolen files or created a backdoor?

To protect agains insider threats, all companies should implement the best practices listed below.

5 BEST PRACTICES TO PROTECT AGAINST INSIDER THREATS:

1. Create a process whereby HR and IT communicate on employee access to systems and information.

2. Make someone responsible for regularly comparing your list of current employees to your list of active directory accounts.

3. Make someone responsible for regularly reviewing access privileges and update them as employee roles and needs change.

4. Categorize your data in detail so you can fine-tune access. Some employees need access to employee names and dates of birth, but they probably don't need their bank account numbers, for example. The more granular your classification, the better your security.

5. Create a separation of duties within IT. No one person, no matter how senior, should have complete access to everything. At a minimum, use what the military calls "two-person integrity." To keep people honest, always have a second person who can see what the first person is doing.

For information on how BTB Security can help you identify **potential insider threats** and set up these best practices, visit:

btbsecurity.com