Business & Company Resource Center

Security Director's Report, Nov 2002 p2

Experts ask: do you have a false sense of security?

(basic security measures, like ID badges, can be easily worked around)

Full Text: COPYRIGHT 2002 Institute of Management & Administration

You instituted a badge system to control access to your facilities. You installed CCTV to monitor the grounds. You purchased tamper seals to keep an eye on assets. And you regularly calculate your vulnerability via assessments to be sure no one ever catches you off guard. With all these elements now in place, it's time to sit back and put your feet up on the desk, right? Not according to experts at the recent ASIS International annual conference in Philadelphia. The hottest security management trend touted there was a warning: You may not be quite as secure as you think you are.

ID badges. "Most ID badges in the corporate marketplace are very easy to counterfeit," warned Dennis Caulley of Caulastics, Inc. (Daly City, Calif.; 415-585-9600; www.caulastics.com). "The corporate marketplace is behind the times." To make his point, Caulley demonstrated just how little it would cost a thief to acquire all the equipment he or she needs to produce a corporate ID badge that could **fool** 95% of the people 95% of the time.

The right computer, the right software, the right scanner: For less than $1,000, crooks can get everything they need to be able to flash a badge that will allow them to walk around your facility without raising an eyebrow. "It's a consumer product now," he noted. And crooks don't have to buy any equipment at all--providing fake identification is a thriving online business.

What's the risk? To date, the fake ID market has been geared toward producing false identification for underage drinkers. But in reviewing dozens of Web sites that sell fraudulent identification, Caulley said he is noticing that these dealers appear to be expanding their market base. PhonyID.com, for example, is adding employee ID badges to its list of products for sale.

What should you do? Now that technology has made corporate badges easy to counterfeit, conduct a new threat assessment to measure the likelihood that someone would want to counterfeit your company's ID badge, suggested Caulley. How likely is it that someone would use a fake ID to gain access to your property, put your employees' safety at risk, or

use your corporate moniker to wreak havoc outside your company?

This last item can be a PR nightmare for high-profile companies. If someone uses "your" badge to gain trust outside your walls, and the media find out about it, they will eagerly report how easy your badge is to counterfeit. If you deem the risk of this occurring to be significant, and employees only use a single entrance, it may be cost-effective and security-smart to add a biometric element to your IDs, Caulley suggested.

Should you run out and buy a new ID badge system? It depends on your assessment, but the answer will most likely be "no." However, when the time does come for you to upgrade your ID badge system, Caulley suggested taking the opportunity to "raise the bar a bit." The best way is to "attack" commercial color printers. "There are some things they can't do as well. Get at those features." When you upgrade, consider hard-to-counterfeit badge features such as:

* Using fine, wavy pastel lines or dots in a line--this is tough for commercial printers to replicate.

* Microprinting--basic machines have trouble with tiny type.

* Using special ink or products that have particle structures that reflect different light.

* Including a hologram.

* Using covert features like invisible fluorescing inks, metmeric inks, or reactive inks.

* Using color on the card stock itself.

* Encoding data within the ID photo.

Conclusion: (1) Recognize that technology is making badge counterfeiting easier. (2) Raise the bar on your next ID system purchase. (3) Stay away from the generic: "Simple designs are simple to duplicate," Caulley asserted. Finally, make sure you have an active security presence: Improving the security of badges is important, but it only makes sense if your people are looking at them.

CCTV. Dissatisfied with the images you were getting from your CCTV system, you went out and bought a new high-resolution camera. You've just improved security, right? Maybe not, according to Charlie Pierce, president and founder of LRC Electronics and LTC Training Center (Davenport, Iowa; 563-324-2199; www.lrc-inc.com).

"The resolution of the camera is only as good as the weakest link in your system," he warned. If you don't understand your weakest link, you may

invest in technology that provides no benefit, be a sitting duck for CCTV salespeople, and have a false sense that you're improving security when you're only wasting precious resources. He recommends that you:

* Learn the technical stuff. At least understand it well enough that you know what questions to ask. "If you're afraid to ask questions, they'll be able to sell you anything." And if you know the basics, salespeople won't be able to bluff you with technical talk. For instance, which sounds like the better buy: Camera A with 600 horizontal lines of resolution or camera B with 250,000-pixel point resolution? Camera B has only 220 horizontal lines of resolution.

* Understand the weakest link in your system. For instance, a high-resolution camera and a high-resolution monitor won't yield a quality picture if the signal also passes through a multiplexer that doesn't have the capacity to make use of it. Take the time to learn the math before shopping. Despite the dizzying number of product offerings, "If you do the math, you can always find the best camera for the application," Pierce said.

* "Don't be afraid to ask for a demonstration." Everything looks good on the trade show floor. Ask dealers to "let me see how it works in my application."

* Learn about signal-to-noise ratio. "It's becoming more important as we go digital," Pierce warned.

* Provide every camera you have with a written purpose. You may only have a few different purposes, but you need to identify--for each camera--why it is there. Only by identifying the camera's purpose can you know whether your system is providing a sufficient quality picture to meet your goal.

Tamper-detecting seals. You may have bought new CCTV technology that is doing you no good and your ID badge may be easy to counterfeit, but at least you can be sure that the extra money you spent on your security seals was money well spent, right? Not according to new research conducted at Los Alamos National Laboratory (Los Alamos, N.M.; 505-667-7414; www.lanl.gov) on 187 different seals.

Security uses tamper-indicating seals in a variety of applications, from cargo security to inventory control to courier services. But spending extra on more expensive tamper-indicating seals may not provide you with better tamper detection. "One surprise we found is that expensive high-tech seals aren't harder to **defeat**," said Roger Johnson, CPP, in reporting the findings to security directors at the ASIS International conference. In fact, on average, their experiment showed that spending an extra dollar per seal (and that's a lot) adds only 1.5 seconds to the **defeat** time. "It thus appears that expensive high-tech seals do not automatically detect

tampering more effectively," the report states.

In fact, all seals are pretty easy to beat, the research found. Researchers could easily **defeat** half the seals they tested in less than two minutes and nearly all of them in less than 10 minutes.

What to do: "Trying to **defeat** a seal is about trying to **fool** people, which greatly complicates the issue," said Johnson. **Defeating** seals is typically easy because companies have lax installation and inspection procedures and because they do not take the time to understand the particular vulnerabilities of the seal they are using (or train security staff in what they are). Improve your inspection procedures, know your seals' weak points, and you can make **defeating** seals difficult or impossible, according to the Los Alamos investigation. "Unfortunately, this combination is rare," said Johnson.

Vulnerability assessments. Finally, a quantifiable vulnerability assessment is a cornerstone of many security programs. But Johnson explained why a mathematical calculation of your vulnerability has limitations:

* You can never "pass" a vulnerability assessment.

* There is often a "shoot the messenger" aspect--those who identify the vulnerability receive the blame for it.

* If you don't want to find a problem, a vulnerability assessment won't find it.

* Security personnel are often far less creative in identifying vulnerabilities than are the individuals who exploit them.

* There are no meaningful standards to judge oneself against.

* Vulnerability is never static--you're always chasing a moving target.

* **Defeats** or security failures are always a matter of degrees.

* There is no clear end point. When is your level of vulnerability acceptable?

* Most security failures are not due to something that a vulnerability assessment can even identify. They are the result of human error.

What to do: You can't do away with vulnerability assessments, of course, but you can realize that a vulnerability "score" will never paint a completely accurate picture of your risk. "Simply because you have a number," Johnson warned, "doesn't mean you should take it too seriously."