Outside Threats Can Get Inside:
Transform Vendor Risk Management to Improve Security

Locks are Most Easily Broken with Keys

Introduction

Certain individuals or groups are willing to go to great lengths to pilfer your company's information and assets. This universal and everlasting truth should be at the forefront when planning and executing protective security measures.

Intense global economic competition, geopolitical uncertainty, the "hacking economy," skills shortages that increase reliance on contractors, and old-fashioned skullduggery mean threats today are more pervasive than ever. It is essential, therefore, that new approaches for vetting contractor and vendor employees be adopted.

Contractors and vendors are ubiquitous: they work across departments, can enter multiple buildings, and have access to most systems. However, given the pace at which business runs, these workers often aren't vetted as thoroughly as an organization's own regular, full-time employees.

Furthermore, when security processes are run internally, they distract from a company's core mission, drain more resources than is warranted, and often are not effective. This costs companies billions, diminishes brand equity and, in some cases, can even harm national security.

An emerging approach promises to counter these threats: Vendor-Led Security Management.

Solution:
Vendor-Led Security Management

A particularly strong model emerging to counter "outsiders on the inside" is Vendor-Led Security Management.

Key elements include:

- **Flexibility:** Program elements are tailored to your company's requirements so that you can "tune the dials" depending on the threat profiles and risk parameters for particular business units.
- **Unified credential:** Issue a high-security ID in use on military bases today that can be recognized by multiple departments, companies, and locations.
- **Pre-clearance:** Strict vetting of contractors and vendors before they are issued a credential and granted access.
- **Ongoing screening:** Automated notification to the vendor organization when an employee no longer qualifies for access.
- **Financial efficiency:** Management is outsourced, expenses are shared across multiple companies, vendors and contractors can be charged for their vetting and credentials.
- **Scale:** Availability of top-tier security to smaller companies that could not otherwise afford to participate.
- **Collaboration:** Easy engagement and participation by both cyber and physical security executives.

Cont.

SureID® Identity Matters™

Outsiders on the Inside Can Do Damage

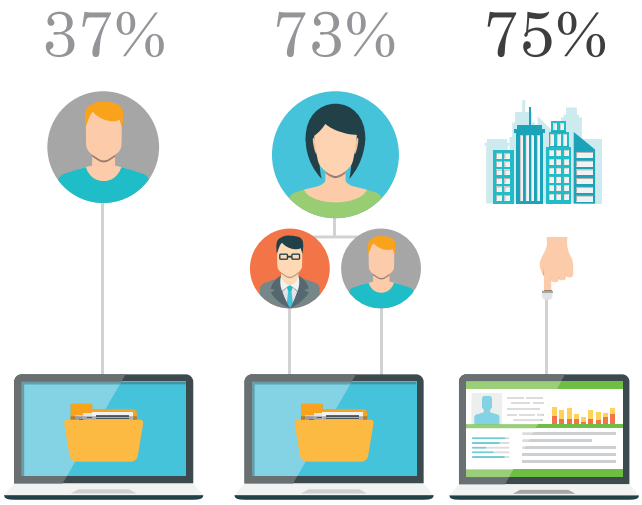
Most security resources today are devoted to stopping unauthorized intruders from accessing facilities or systems. This is understandable given how difficult it can be to lock down large, far-flung facilities or defend systems from hackers. However, it is not sufficient.

It's a fact of business that companies must grant access to contractors and vendors. Everyone from delivery and maintenance personnel to professional services and IT experts are allowed into a company's most security-sensitive locations. But risks are self-evident: Edward Snowden publicly leaked thousands of classified documents to the press while working for a highly reputable firm under contract to the NSA. In fact, he sought that job because the contractor's reputation was so good that its access was effectively unfettered.

Could these scenarios happen in your company?

- A building contractor conducting needed repairs or upgrades after hours steals equipment or files.
- An IT technician performing infrastructure upgrades uses a thumb drive to siphon data.
- A landscaper leaves a distant gate unlocked.

Chances are strong that the answer in each case is "yes."



Furthermore, according to a recent survey, 37% of companies said they doubted contractors would self-report an incident perpetrated by one of their own; that number jumps to 73% when the offending party is under contract to the contractor. Of even greater concern, 75% of respondents think vendor-involved security incidents will continue to grow.

Before and after breaches occur, systems must be established to detect, minimize, and mitigate potential threats. Many existing physical and cyber security resources and processes can be brought to bear, but not all.

For the scenarios above, Vendor-Led Security Management would significantly reduce the likelihood that 1) bad actors would be granted access in the first place, and 2) make it more likely that access would be denied for those who become threats after initial vetting.

Where Do I Start?

Start with this list of questions:

- Do the legal agreements I have with my vendors require a background screen?
- Does my organization have a system in place to properly vet contractors and vendors before they are granted access?

Cont.

- If contractors and vendors vet their own employees, is my organization performing audits to ensure my standards are adhered to?
- Are these populations subject to ongoing vetting by the contractors themselves or by my organization?
- Are contractors accepting our requirements, even if they cause duplication of effort for other companies they serve?
- Am I able to stay current with advances in security, or are software and hardware patches taking an inordinate amount of time and attention?

After getting through this list, there are other key aspects to consider:

- **Scale:** If I outsource, can my programs scale?

  With vendor-led security management, contractors and vendors pay for their own vetting and credentials which means the program can grow person by person, by the thousands, or somewhere in between, and never hit a roadblock.

- **Fairness:** Will I be the priority, or will those paying for vetting and credentials be favored?

  By definition, the security provider serves both companies and their contractors; this promotes fairness and makes it easier to push for performance and cost improvements.

- **Policy Flexibility:** Will it be easier for me to design and carry out identity proofing and vetting?

  By utilizing an outside organization to manage the identity assurance lifecycle from beginning to end, reliant organizations may be less likely to be perceived as treating their outside vendors like employees.

- **Vendor Stature:** Will my contractors and vendors be OK with this approach?

  By showing current and future clients they can fulfill and maintain broad industry standards, contractors are able to demonstrate increased credibility and capability.

Outsiders will never stop trying to get inside to do harm. Take an important step to make sure you're only giving access to people who should have it.

To learn more about SureID, the leading provider of high-assurance identity solutions, visit: **www.sureid.com**

SureID® Identity Matters™