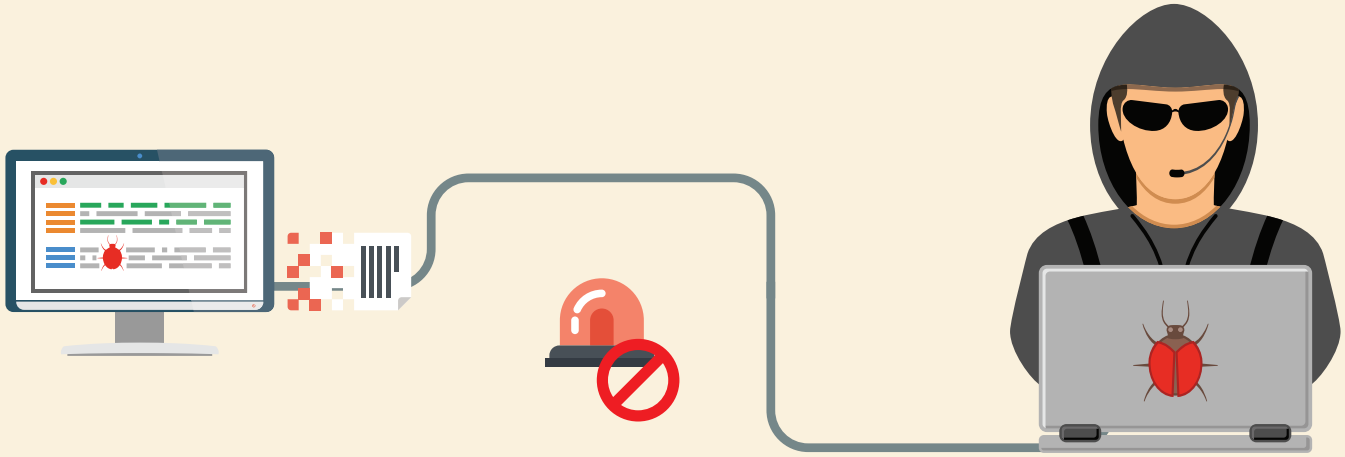
Protecting Against Hackers Inside:
How Organizations of Any Size Can Now Vet, Track and Consistently Validate Vendors and Contractors Before or After They're Granted Access



Introduction

Recently disclosed high-profile hacks against the Democratic National Committee, the New York Times and Yahoo! have drawn increased attention on attempts by outside malicious actors to disrupt crucial business processes. However, more than half of all global data breaches were caused by:

- Negligent employees and contractors (who themselves are so much more numerous as skills shortages get more acute, offshoring gets easier, and specialization gets more desirable)
  or
- IT and business process failures

Those data breaches, no matter the culprit, can be incredibly costly. In 2015, British insurance company Lloyd's found that hacks cost global businesses $400 billion a year.

These vulnerabilities suggest that a new approach to vendor security is well-justified.

Auditing Your Vendor Management Security Framework

Organizations with an ever-changing list of vendors and contractors who handle sensitive information must ask the following 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?
- 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?

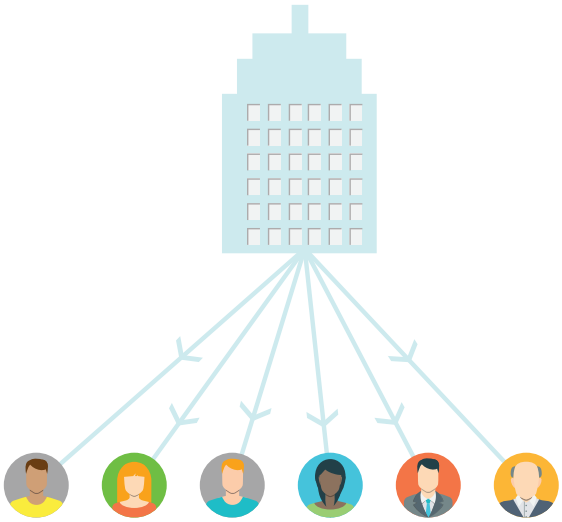
Cont.

SureID® Identity Matters™

Answering "no" to any of the previous questions suggests that the organization in question must take additional steps to properly mitigate internal risks that are a significant cause of data breaches across the globe.

Two Approaches to Security Management: Closed-Loop vs. Vendor-Led

Two vendor management models have emerged to protect security. The first is closed-loop vendor management security. It represents an internally managed, end-to-end security framework to vet and re-check contractors and vendors as required by the terms of the respective relationship. This is a traditional method in wide use today.



Closed-Loop Vendor Management Security

Advantages

- Organizations can define the terms of the acceptance criteria and adjust as they see fit, ensuring quick responses to constantly evolving needs and issues. This may include screening for certain professional qualifications in addition to identity verification.
- Organizations have full control over every aspect of the system, even when outsourcing the function.
- Complements existing identity and access management (IAM) solutions.

Drawbacks

- A closed-loop model requires significant investment up front that only large enterprise organizations can typically afford.
- Vendors and contractors are subject to multiple processes and checks.
- Staying current with industry advances is a challenge, particularly when security is not core to the organization's mission.

The Future: Vendor-Led Security Management

A particularly strong and more cost-effective model 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.

Vendor-Led Security Management

Advantages

- The model provides small, medium and large organizations access to enterprise-level vendor management risk mitigation without the need to invest in the infrastructure required to support a closed-loop system.
- It gives participating vendor organizations a potential competitive advantage in that they can show trustworthiness through an industry-accepted standard.
- External management of these processes ensures that emerging trends and technologies are recognized and incorporated whenever appropriate.
- As the program can be purchased on a per-credential basis, the vendor-led model is scalable to organizations of nearly every size on both sides of the relationship.
- Since the outsourced security specialist is in a business relationship with both vendors and reliant organizations, both sides can expect transparency along with fair and equitable treatment.
- Successful completion of robust security programs eliminates a hurdle for vendors to win business.

Outsourcing Vendor Identity Proofing

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.

Furthermore, an audit trail is available to ensure a proper background screen is actually occurring, thus eliminating reliance on vendor guarantees that proper screening is being conducted. The outsourced security specialist provides this information to both parties per the agreed terms of contract, promoting transparency throughout the process.

When Vendor Security is Done Properly, Everyone Wins — Except Bad Actors

Vendor-Led Security management offers better security at a lower cost. When assessing system vulnerabilities, it's clear that unapproved vendors represent a significant threat— the Vendor-Led Security Management model described above offers a new and powerful way to counter this threat.

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

Protecting Against Hackers Inside:
How Organizations of Any Size Can Now Vet, Track and Consistently Validate Vendors and Contractors Before or After They're Granted Access

SureID® Identity Matters™