

Circle of Trust

By Jason Ezratty and
Christopher Minnick

Vet and inc



In the hit movie, *Meet the Parents*, a retired CIA agent finds out that his daughter's boyfriend knows of his CIA past, and says, "You are now on the inside of ... 'the Byrnes family Circle of Trust.' I keep nothing from you; you keep nothing from me."

Many contingent workforce program owners describe the state of their company's information security with regards to contingent workers as: "scary." After all of the legal agreements, background checks and authentication methods corporations employ, they still need to trust people on a gut level. We rely on our interviewing skills and intuition to raise red flags on questionable candidates but we know these screening measures are not flawless.

Many argue that the increasing usage of contingent workers amplifies exposure to trust-related risks. Given the relative transience of contingent workers, securing facilities, systems and confidential information are harder and more burdensome than ever. Thus, it is up to you to enlist onboarding workers to your Circle of Trust, considering all the sensitive things they see, learn and touch while on your premises.

COMPLEX PROCESSES

Corporate employees sign contracts, log in to computers using passwords, lock our desk drawers, show a badge to security — all because employers don't know whom they can trust. With all of the brainiacs developing information systems out there, surely our data and facilities access points are secure, right? Of course not: systems-level information security controls often leave holes, too. Even if your systems were configured properly, they are used and administered by people. Unlike machines, people are trained, not programmed. We ask them to use our systems correctly but what they actually do often varies.

Despite the highly sophisticated encryption and authentication methods available, managers of contingent labor are often more focused on the immediate goal of getting their project com-

pleted than the less tangible threat of intellectual property asset loss. While laziness is often to blame, sometimes it is the process that is at fault.

For example, a Web form requires an employee ID in order to generate a new systems login for a contingent worker, but in some cases contingent workers don't get employee IDs. Or, maybe they get an ID but it takes two to four additional weeks, delaying the project for which the contingent was brought on board. Or, maybe they get an employee ID, which the manager or vendor reuses in subsequent engagements with other people.

program for Apple, which is about to launch its iconic iPod, except in this scenario, a contractor doing short engagements for area companies unintentionally spread the word about Apple's focus on the color white in launching the new brand. As a result, two then-formidable competitors also released white devices with white ear buds. Even if this leak of confidential information only slowed the pace of iPod sales by 20 percent, it would have cost Apple billions of dollars in revenue.

Or imagine you're running the CW program for Glaxo-SmithKline and a temp who did routine bench science describes

Protect your contingents while safeguarding company systems

It isn't surprising that simply getting through the process defines the task more than the intended goal of the process itself. Success is measured by how quickly they are able to arrange access for their contingent worker, not by how secure or compliant the result is. Many managers think, "Why do they make this so difficult?" You'll even hear, "If we can't trust Bob the temp DBA, why did we bring him on for the next six months?"

HIGH STAKES

In today's global, techno-charged, competitive arena, the stakes are higher than ever. You count on your workforce to help you win this competition on all fronts, from sales to delivery to customer service. Given the thousands of individuals that currently comprise your workforce, it's safe to assume at least some are leaving on a daily basis. Information leaks are more likely to happen by accident, as a worker migrates from one corporate IT environment to another, than by malfeasance. While passive, it is no less damaging.

As such, an important element of the trust equation is choosing what information is worth sharing, before needing to worry about who else it might be shared with. In corporate security, trust (a.k.a. "clearance") is often described in terms of areas (i.e. what you need to know about), levels (i.e. how much you need to know), effective period (i.e. how long you need access to that information), and portability (i.e. where/how you are authorized to take this information). When considering the various types of roles being performed by your contingent workers and thinking about their level of access to information does anything register as "scary?" Of particular concern is the question of portability. While the Internet has enabled us to get more done from more places, it also means that vast quantities of data can be downloaded quickly and without a trace.

Consider some hypothetical, but entirely probable scenarios. Imagine in 2001 you were running the contingent workforce

the types of experiments he was performing at his next interview with your competitor. While this individual may not have even been aware of the actual purpose of the research, a savvy hiring scientist might discern what your company is working on based on that information. In pharmaceuticals, it is critical to keep such information confidential because long development timelines make your duration of novelty a critical competitive differentiator.

Finally, imagine if Bob, the DBA you hired to implement your shiny new customer relationship management (CRM) system, sold or otherwise leaked data to competitors. Nowadays, several gigabytes of data can be stored on portable media such as memory keys. From a single record to an entire database, data can be deleted, or otherwise compromised (e.g. virus or other such cyber-parasite). While it's hard to understand why someone would do this, as the contingent workforce program owner, it is your job to conceive of cost-effective means to mitigate against it.

If somehow it were discovered that any of the three scenarios were the result of contractors leaking information, you would likely be in for some heat. While the department-level treatment of the information in question is likely the root of the problem, it wouldn't be surprising if you as the CW program manager became the scapegoat. As we've all witnessed, blame is typically assigned to the easiest target, not the most probably culpable.

TRACK YOUR TEMPS

Your best bet to avoid any such scenario is to vet your contingents, which begins with properly identifying them prior to onboarding. If you cannot accurately identify prospective workers then you are immediately handicapped from knowing anything about their past. You also run the risk of creating a second record in your database for one individual. However, to do this job right you must consider that the individual you are

trying to identify was previously a worker of a different type (e.g. former employee returning as a contingent worker). As such, a comprehensive tracking system universal to all worker types is vital to success.

When analyzing this problem on a global scale, one quickly realizes that first and last name combinations do not suffice. With the number of Smiths, Guptas and Changs in the world, you are likely to find a number of matching first and last name combinations of different individuals. Furthermore, parsing Joe Smith from Joseph Smith will not be sufficient to declare these individuals as distinct.

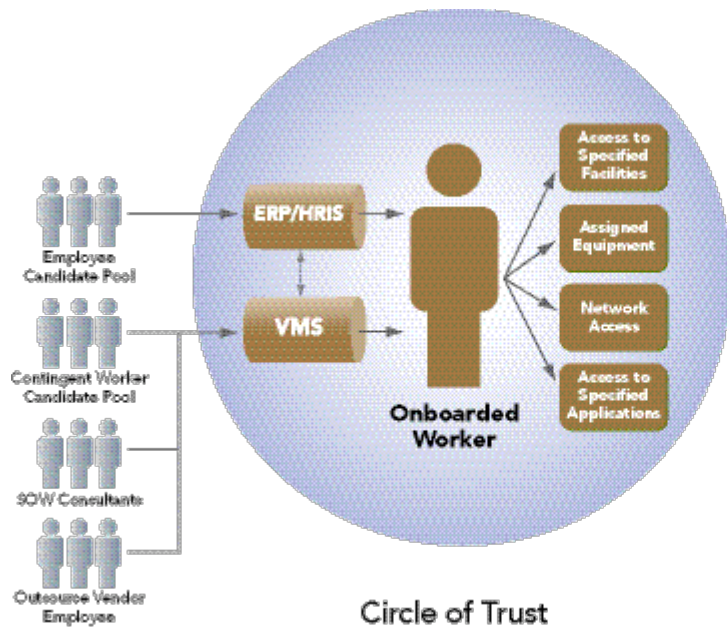
In addition, in countries outside of the English-speaking world, names are often phonetically spelled since we have a different set of characters that compose our written language. For example, the Chinese surnames Chang, Wang, Wong and

Huang are often spelled with the same character. While some database products can store names in native characters, many application developers do not take advantage of this. The danger here is that if a returning worker is entered into your system under a different

phonetic translation into English you may be hampering your ability to identify the individual's data from previous assignments.

This is especially difficult in areas that do not mandate use of a national identification number or whose privacy protection laws prohibit or make it impractical.

In the United States, this can often be solved by requiring a social security number (SSN). However, many recruiting firms are reluctant to provide accurate SSNs until the candidate has already been selected, if at all. Their claim is that this applicant is their "inventory," and companies might otherwise go around the staffing agency and approach the candidate directly. Whether this is a founded concern or not, the results are polluting your databases with information that is making a mess of reporting and invoice auditing efforts. Vendors and candidates need to be able to trust companies with their important infor-



STEVE CARAMIA

Research a contingent before trusting him.

mation, too — it is all part of the circle of trust.

Providing a partial SSN plus name combination is an attempt some staffing companies make at compromise, but that can add time and complexity to onboarding cycles when trying to parse candidates with similar names and a matching partial SSN. While relatively infrequent, in large programs it happens more than you would expect — especially considering that names or partial SSNs often are entered incorrectly in the first place.

However, a surprising number of countries do not mandate national identification numbers, which makes your prospects of going global that much harder. Even in the United States, while the SSN is used as a unique identifier, registering a baby with Social Security is not compulsory. While the vast majority of American parents do so in order to receive the dependent child tax benefit, poor and uneducated segments of the population often go without.

While the potential lack of a SSN shouldn't be an issue for contingent workers sourced through staffing agencies, it may pose an issue with landscapers, cafeteria workers and other outsource contract arrangements. This is referred to by some as the shadow workforce, and can include illegal immigrants who often do not have SSNs — but sometimes purchase SSNs illegally — complicating our identification problem even further.

WHAT TO LOOK FOR

Assuming you can accurately identify a worker, there is still much work to be done. First, one can look into a prospec-

tive worker's assignment histories. What roles has he performed in the past and as what worker type? If a previous contingent worker is returning, as a contingent or an employee, were there any performance quality notes? A pay rate or bill rate to compare against (from the same or a different supplier)? There are all kinds of information someone onboarding a worker might find — if it were being captured and stored electronically.

Setting up such a system requires that one endure the pain of systems integration. While a couple of the enterprise software providers are positioned to do so, to date, no single software provider has demonstrated the ability to assume the full set of features represented by HR information systems, enterprise resource planning and vendor management systems. Making your hard day harder, your over-worked Management Information System (MIS) staff will likely put this project in queue somewhere on their roadmap ... perhaps for release in 2012, assuming no delays. Finally, once your universal worker data have been consolidated, you need to relay this information to your badging and network access authorization and authentication systems to finally realize the intended benefit of actually controlling

access to systems and facilities.

Then, you'll need to figure out who will own and manage this multi-worker-type function, including whether contingents should have access to it. If you already have a cross-functional contingent workforce program in place, this is a good starting point because the stakeholders tend to be the same.

CONCLUSION

Naturally, there are limits to what is appropriate that every organization must set for itself. What is deemed excessive for one company's culture may be inadequate for another. Regardless, every organization has the need to safeguard their systems and facilities and should consider how an increased use of contingent workers could impact their vulnerability to property or information losses. The boyfriend in the movie turned out to be a great guy; however, in the contingent world, that may not always be the case. 🌐

Jason Ezratty and Christopher Minnick consult Fortune 500 companies on contingent workforce strategy initiatives such as program design, VMS/MSP selection assistance, and performance metrics analysis (www.brightfieldstrategies.com). They can be reached at jezratty@brightfieldstrategies.com or cminnick@brightfieldstrategies.com.