

Securing 'Corporate Ghosts'



Table of Contents

Foreword	3
Executive summary	4
Research methodology	5
Network user complexity	6
Perimeter control preoccupation	7
'Corporate ghosts'	8
More identities, more 'ghost' headaches	9
Identity-based control	10
Conclusion	11
ConSentry top tips	12

Foreword

As we enter 2007, analysts continue to emphasize security is a key priority for IT departments. Even allowing for the significant investments already made, it's not particularly surprising to see security high on the IT agenda when you consider the scope of vulnerabilities that businesses face today in protecting their corporate assets.

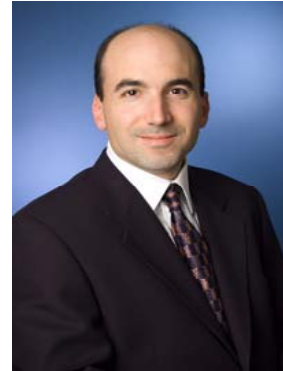
However, we wanted to get a deeper understanding of the state of LAN security in large corporations. What are the current attitudes to network security and how are they affected by the changing dynamics of business operations? Are there any overlooked holes in security or is today's LAN security sufficiently robust to deal with whatever 2007 brings?

We commissioned Loudhouse Research, an independent research consultancy, to investigate and analyse the state of play on our behalf. In doing so, we uncovered the phenomenon of 'corporate ghosts,' guest contractors or employees who are able to roam potentially sensitive areas of corporate networks without being detected. As networks increasingly accommodate different types of network users, the prevalence of these 'ghosts' also increases.

In today's business climate of spiralling internet threats, increasingly sophisticated cyber crime, and corporate fraud, it is imperative for every user on the corporate network to be clearly identified and constantly monitored. The need, therefore, to 'exorcise' these 'ghosts' and secure applications and resources based on identity and user role is becoming more and more critical.

The research suggests IT departments have a unanimous requirement for identity-based network access control, but this demand brings with it some key challenges. First, integrating such security measures into what is likely to be an already complex infrastructure is a major consideration. Second, increasing IT security has historically always meant decreasing network performance, and LAN-based demands make this concern even more serious. Last, any identity-based control must ensure a balance between protecting corporate assets from users on the LAN and allowing those very users to do their job as efficiently as possible. Tying user identity to activity and controlling where users can go, without compromising their productivity, the network's performance, or the IT department's resources sounds hard but is actually easier than you may think.

We exist to help businesses protect themselves by allowing them to control access on their corporate networks, and we're heartened to see so many IT executives citing these requirements. We hope you find this report as insightful as we did and that it helps you to better prepare yourself against any 'corporate ghosts' that may be roaming on your network.



Dan Leary, Vice President of Marketing,
ConSentry Networks

Executive summary

Increasing network user diversity is raising concerns that there is a need for a more dynamic approach to LAN security. The following report tackles this issue, advocating an identity-based approach to managing users on the network.

The key drivers for focusing on network security from a user perspective come from the level of transitory, or non-permanent, workers who access network environments on a daily basis. The research found a significant majority of respondents seeing the following groups as a threat to the network:

- Temporary workers (62%)
- Guest users (54%)
- Contractors (51%)

With 82 percent of businesses in the survey saying they have moderate to high levels of non-permanent workers accessing the network, it appears that the changing shape of the workforce is a contentious issue for security professionals. Further highlights from the research are as follows:

- 87% of respondents state that they have multiple levels of user access
- 82% of respondents recognise the need to increase network security
- 95% believe there is an increased need for the use of identity-based control
- 41% of businesses do not have up-to-date network access
- 65% acknowledge that network access is becoming more diverse and difficult to manage

Despite the fact that 75 percent of respondents claim to have a policy to ensure guest users cannot spread malware via the LAN, it is evident from the perceived need to increase network security that existing policy is falling short of expectation.

The report suggests that the risk presented by 'corporate ghosts,' users roaming the network uninhibited by barriers and boundaries, is something enterprise network managers need to review. Without sufficient security provisioning to control diverse user groups, the risks of information loss, or the inadvertent distribution of malware from this 'ethereal' user group, companies are undermining their own efforts to provide a safe, controlled, and efficient network environment for the organization as a whole.

The survey concludes with the recommendation that security professionals and network managers need to evaluate the current nature of network control in context of a diverse user community and an increasingly flexible IT infrastructure. The proliferation of means by which a network can be accessed, both in terms of device and location, combined with a mix of distinct business-user levels and non-permanent workers, creates conditions for high risk if managed incorrectly.

Research methodology

The research was commissioned by ConSentry and undertaken by Loudhouse Research, an independent B2B consultancy. Loudhouse interviewed 200 security and network professionals during November/December 2006. Respondents represented businesses of at least 250 employees, with the majority of respondents coming from organizations of 1,000 or more employees. [Figure 1].

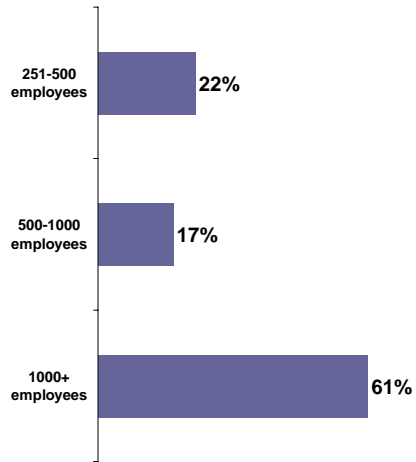


Fig. 1: Research sample

Network user complexity

It is a given that most of today's large organizations operate a sophisticated network environment, but it is also important to understand the 'typical' network that forms the basis of the findings for this research. Figure 2 uncovers the significant levels of diversity that most security and network professionals face, purely from an internal/LAN perspective. Respondents were asked to score the relative presence of each network characteristic on a scale of 0-5, with the following results.

Multiple levels of users access

87 percent of respondents state that they have multiple levels of user access, making it the first and most significant element of network security. It is worth noting that multi-layer access does not always follow a typical pyramid of hierarchical need. Increasingly, levels of access take on more of a matrix model, with departmental, divisional, and skills-based roles dictating where access should be applied.

Multiple sites/offices

Though most large businesses will have multiple sites, it is again interesting to note that 85 percent of businesses have a highly distributed geographical network. This stretches the security need in another direction. The wider the distribution of network access, the harder it is to provide consistent provisioning across the network. The network 'footprint' places a heavy burden on internal resources to support and maintain operations.

Mobile access

Over the past five years, many issues surrounding the pain of standardisation for mobile devices on the network have been overcome. It's easier to manage mobile devices today, demonstrated by the fact that 94 percent of businesses support moderate to high mobile usage. Unfortunately, mobility also presents significant security issues, from device theft through to dynamic access and identification requirements to ensure that the wireless infrastructure is not abused.

Temp/guest access

The phenomenon of non-permanent workers accessing the network cannot be underestimated as a potential security threat. As stated later in the survey, it is widely acknowledged that security risk increases with this group. This does not suggest that non-permanent workers are more of a risk as people, but they are a particularly vulnerable group in terms of malware and inadvertent security breaches, simply by the nature of their role and their relationship with the business. Of course, if the non-permanent worker also works across a mobile, multi-site, multi-level access environment, the security challenges are compounded.

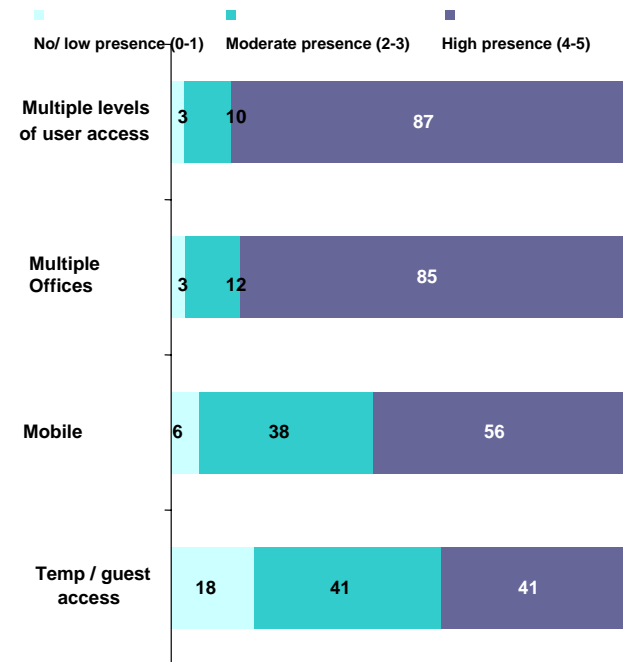


Fig. 2: Network characteristics

Perimeter control preoccupation

As Figure 3 shows, virtually every organization today has multiple security measures in place from first-pass corporate firewalls (97 percent) to identifying users as they log onto the network (93 percent). The point of interest here, however, is that once users are allowed in, how secure are those organizations?

Imagine IT network security in terms of the team of doormen at a large nightclub. Security provisioning does not rely solely on checking people at the door (i.e. perimeter control) but rather on total security – and visibility – inside the club as well. For example, guests at the turnstile may behave completely differently once inside the building, security checks may not detect all potential threats on entry, and the clientele, even if members of the establishment, may not behave consistently each time they enter. Therefore, it is essential that security also monitors the behaviour of guests throughout all of their visits.

In the same way, IT networks must facilitate comprehensive traffic visibility, making post-admission checks as important as pre-admission scanning. Figure 3 shows that the majority of businesses have pervasive ‘rigid’ security measures in place, but only 36 percent take any notice of traffic security once filter checks have been passed. It appears that the majority of respondents are happy to have most of the ‘muscle’ at the door but have a potentially reckless disregard for behaviour post-admission. Perhaps more alarmingly, over 40 percent of businesses do not scan for device authentication pre-admission despite the fact that 94 percent of them have moderate to high levels of mobile access across the network.

Figure 3 describes a typical network environment where the emphasis is on the protection of data rather than on a dynamic understanding and control of the user. Of course, the majority of networks will ask for user authentication to enable access, but this is a very basic security measure and one that can become very difficult to manage in terms of directory verification.

Figure 7 (page 10) illustrates the vulnerabilities of modern corporate network security arising from today’s operational challenges; 41 percent of organizations do not even have an up-to-date network access policy *that meets their own expectations*. In organizations with more than 1,000 employees, the figure is over half (54 percent).

Prioritising the understanding of user identity over data/file security will have a natural influence on an organization’s approach to network strategy, which should facilitate a more secure and more efficient method of running the network itself. However, as we will see in the next section, it is the diversity of today’s network users that presents the major challenge to LAN security.

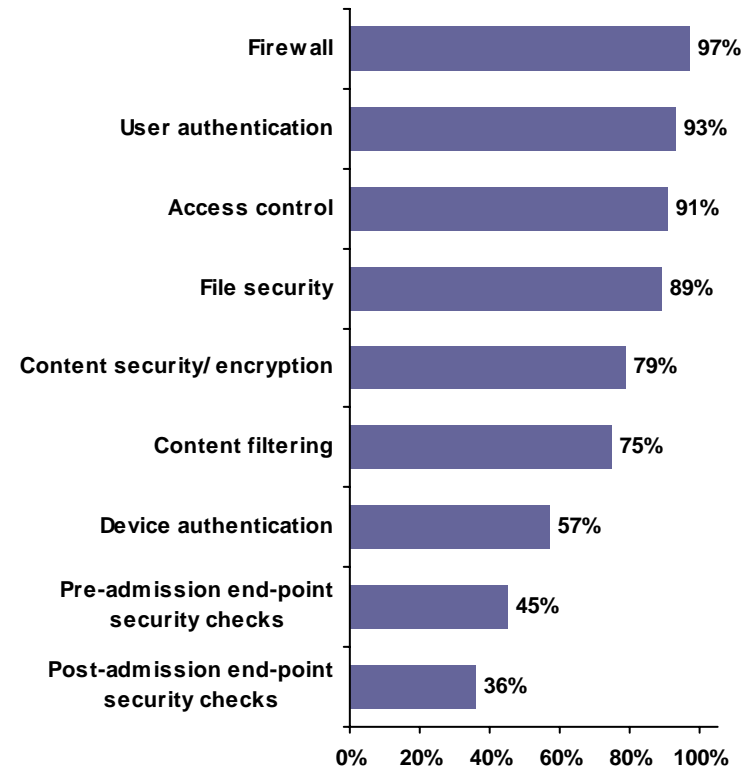


Fig. 3: Functions present on the network today

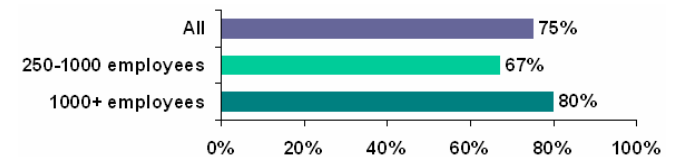


Fig. 4: Percent of companies with a policy/process to ensure guest users/contractors cannot spread malware via the LAN

'Corporate ghosts'

It is interesting to reflect further on the nature of the modern workforce. In little over a decade, the typical workforce has fundamentally changed. A large organization today is an IP-enabled group that depends almost entirely on electronic communication and file exchange. Not only has it become more culturally diverse, but it is also a far more transitory group, both in terms of geography and job roles.

In many sectors, outsourcing has also become a pervasive component of corporate strategy, widening the user community further. As a result, temporary and contract working is present in most businesses. From the survey [Figure 2], 41 percent of businesses accommodate a high level of temporary and contract workers and 41 percent a moderate level of the same groups. It is also not uncommon for clients and guest users to 'plug in' and borrow corporate network resources to work off-site.

Figure 5 shows that all these non-permanent user groups are considered more likely to be a potential source of data loss than internal employees. Over half the surveyed IT staff associates a high risk of data loss with temporary workers, guest users, or contractors. It is important to understand that data loss itself can manifest in many ways – it is not simply a case of pre-meditated theft! Data loss can result from the erroneous removal of commercial information by an external third party, or, perhaps more commonly, the inadvertent spread of malware from a third party's laptop.

This subtler type of threat is why understanding the user 'posture' and being able to provide a clear audit trail of resource access for each network user is critical to tightening network control. Not only does it help with pure security measures, but increasingly it is becoming an aspect of legal compliance to ensure that monitoring is both watertight and auditable.

The challenge with many existing network access regimes is that guest users are often left to roam the network and pass, like ghosts, into prohibited, or unnecessary, areas of the network environment, without sufficient tracking in place.

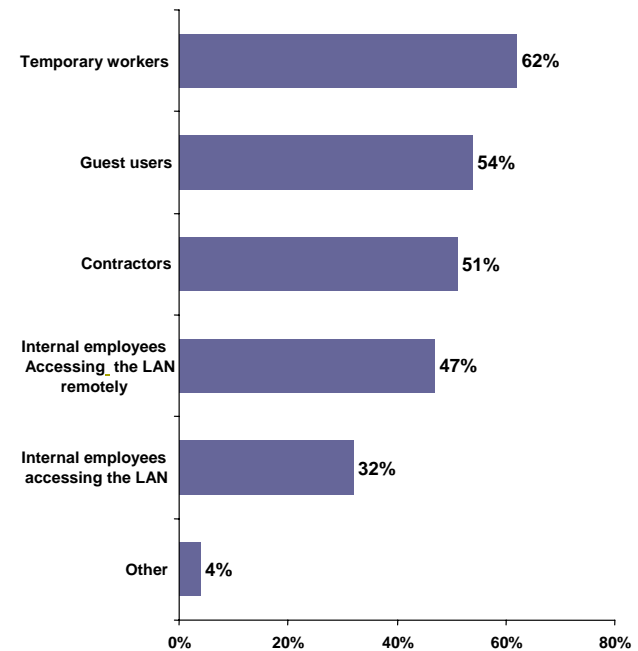


Fig. 5: Groups that are considered to pose the biggest risk to the network in terms of potential sources for data loss

More identities, more 'ghost' headaches?

Figure 6 shows the extent to which respondents agree to two statements: the need to increase levels of security to respond to escalating threats surrounding network access (82 percent) and the range of users accessing the network becoming increasingly difficult to manage (65 percent).

Although 75 percent of respondents claim to have measures in place to prevent malware spreading across the LAN [Figure 4], only 59 percent are actually satisfied with their existing security policy [Figure 7] and acknowledge that more needs to be done. Herein lies the ultimate conundrum with security strategy; it is rarely a done job. IT has the desire to stay ahead of the game, the predicament of needing to keep up, or the perennial need to adapt measures to organizational change.

The interesting point with this particular facet of IT security is that it is not necessarily driven by the 'cat and mouse' game of virus threats and sophisticated hacking practices. From the perspective of network access, the key concern revolves around user diversity. Having to contend with multiple types of users is causing many IT departments to consider how to develop a meaningful, future-proof strategy that facilitates productive workflow while maintaining network control.

Such a diversity of user identities across modern corporate networks goes some way to explaining why 4 out of 10 respondents in Figure 7 believe their security policy is either failing to meet expectations, requires review, or is simply not in place! Within all these respondents there will be those that already have highly effective measures in place but feel the need to do more, as well as those that consider everything to be satisfactory when the reality is that security is in need of immediate attention.

When you consider the practical challenges posed in containing these 'corporate ghosts' on the LAN, and the escalating risks they represent, then the overwhelming need to better manage network access is understandable. With such a high level of acknowledgement that more needs to be done here, it is important to understand how IT professionals are currently keeping tabs on their 'corporate ghosts.'

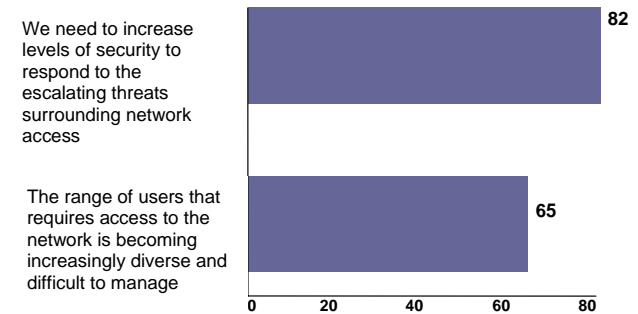


Fig. 6: Shows percent of respondents agreeing (4)/strongly agreeing (5) on a scale of 1-5 with each statement

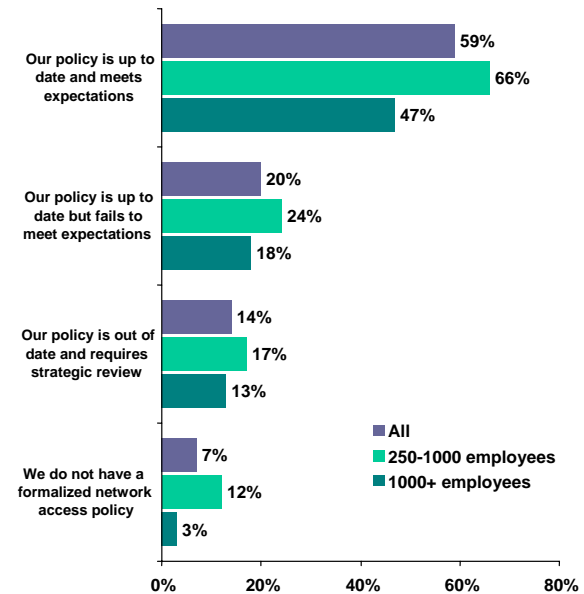


Fig. 7: How would you describe your existing network access policy?

Identity-based control

Figure 8 highlights two issues for people trying to address network access for diverse groups of users. In asking how businesses approach network access for temporary/guest users, it shows that the audience is split across ID and directory verification, the use of a virtual LAN environment, application-specific control, or no specific measures different from those employed for regular users.

With approximately a quarter of the responses in each category, it suggests that there is rarely a one-fit solution for all businesses. Companies are experimenting with different approaches depending on the corporate need and the risk associated with guest users. There is perhaps a greater concern for those businesses yet to establish different access models for different groups, which begs the question of what level of monitoring or network provisioning is in place. By not differentiating by type of user, this group is more susceptible to hosting 'corporate ghosts' than the other respondents, as they potentially allow users to roam the network without restriction.

Each choice of guest-user access control will be determined by the level of security risk associated with the group and the level of access that is needed. Highly skilled contract workers, in particular, need wide-ranging network access at high levels, which should be mirrored by the sophistication of network access control.

Interestingly, almost 1 in 4 respondents in Figure 8 admit to having no specific controls in place for contractors even though 41 percent provide these 'corporate ghosts' with network access [Figure 2]. Sensitive to the potential threat of 'haunted' networks, a nearly unanimous 94 percent of respondents believe that there is an increased need for identity-based control in order to restrict access to critical data [Figure 9]. So if such obvious security gaps exist in corporate networks and the desire for more control is clear, why isn't it in place?

Figure 10 gives some indications as to what prevents network access control best practice. Evidently, resources are a major factor, with 45 percent of respondents citing resources as a barrier, but user diversity is considered almost equally important (44 percent). This data provides even stronger evidence that changing workforce demography and working patterns are a principle reason that security professionals are seeking new approaches to network access control.

Today's IT departments are being required to map security provisioning to a changing workforce, constantly having to react to external changes. This makes demonstrable IT value hard to establish. The corporate strategy to control network access therefore needs to factor in such future challenges as user groups becoming more diverse, mobile devices become more prevalent, malware becoming more sophisticated, and so on.

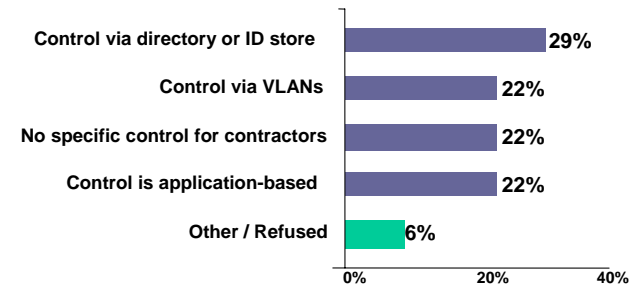


Fig. 8: How do you control LAN access for temp user groups?

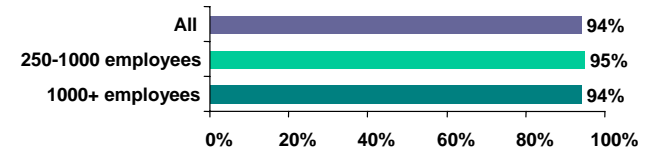


Fig. 9: Perceived need for use of identity-based control

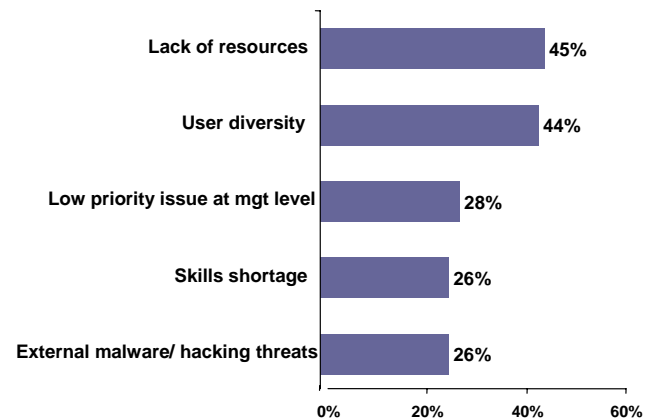


Fig. 10: Key factors impacting network access control today

Conclusion

The common misunderstanding that many businesses have of IT is that the network dictates the way the workforce functions. Tactically, this may be the case; for example, if the network goes down, the workforce comes to a halt. However, if network strategy fails to take into account the evolution of working patterns, as well as internal and external security threats, the only thing it dictates is the scale of the shortfall in meeting corporate expectations.

The “Securing ‘Corporate Ghosts’” survey, commissioned by LAN security expert ConSentry, shows that a representative sample of large organizations understand that user diversity is increasingly security risk. This manifests itself in the form of ‘corporate ghosts,’ which are a result of modern business operations and pose a substantial threat to an organization’s assets. The number of such ‘ghosts’ is undoubtedly on the rise, and businesses cannot afford to allow them to roam freely on their networks - and that issue presents a productivity quandary. The question is how best to respond to the changing dynamics of network control, while allowing full network access to legitimate users?

Network Access Control (NAC) is an increasingly established buzzword among IT professionals, mirroring concerns about identity-based security controls. However, meaningful security solutions do not result from buzzwords alone, and a thoroughly considered security strategy is the principle starting point for successful network security. The research presented within this report presents a typical view of an organization’s security profile and the issues large businesses are currently experiencing. Though there will be evident differences among companies and business sectors, many of the findings will resonate with security professionals across the country. The key thing is what to do next.

With the broadening of the security threat, driven by user diversity and device proliferation, comes a breadth of potential avenues to explore in order to find a fitting solution. The first consideration is to establish what is considered to be a security risk for your business. This step should precede any other security-related decision. As an IT department, the job in hand is to reduce risk, add value, or remove operational cost from the business. If the identification and prioritisation of security risk is not established, measurements of success will be near impossible.

Risk evaluation does not have to be a weighty process in itself. It can start with a few simple questions: what is the network access priority? Is the key area of focus endpoint security, user authentication, or the enforcement of access controls? Where is the level of importance associated with each aspect of security? Does access control apply to every single port on the network, or are there key areas where it should reside?

As a busy IT professional it may feel like you do not have time to think about policy, but security, potentially more than any other aspect of IT planning, requires a policy-first approach.

ConSentry top tips

To help with next steps, ConSentry has outlined key considerations that should provide a constructive starting point in tackling some of the issues raised by this research.

- Establish your user landscape to help prioritise network security measures – are you a company with high employee turnover? Do you rely heavily on temporary or contract workers?
- Establish or update policies for guests, temporary workers, and contractors – train users on how to help these workers gain access without compromising longer-term security, such as by sharing their own passwords
- Review the identity store for accuracy – ensuring long-term contractors are included, and all user groups are up to date, will simplify the rollout of identity-based controls
- Identify at-risk data or resources that ‘corporate ghosts’ have or could have manipulated or compromised – discuss with management a plan to layer-in controls over these users and this data
- Establish cross-departmental and inter-departmental buy-in for changes in approach to organizational security; operational, security, network, and applications professionals will be affected, so support from all areas is critical
- Target ‘bitesize’ areas of the network or user community for early adoption – tactical pilot projects can provide useful learning curves and facilitate short-cuts to strategic success
- Deploy network-based controls in the most sensitive areas first – conference rooms and “hoteling” cubes (designated for roving users) provide a good starting point
- Broaden network-based controls to more pervasive deployment so that all access is controlled – ensure traffic on every port goes through a LAN security check

For further information on reviewing network access strategy, or to discuss the findings from the ‘Corporate Ghost’ research, please contact the following:

- Billy Hamilton-Stent, Research Director, Loudhouse, +44 845 408 4740, billy@loudhouse.co.uk
- Michelle McLean, ConSentry Networks, (408) 956-2100, mmclean@consentry.com
- Shannon Malliet, Engage PR, (510) 748-8200 x309, smalliet@engagepr.com