The Trust Paradox

Access Management and Trust in an Insecure Age

Organisations are struggling to cope with two obvious forces: the need to maintain trust, and the reality of cyber breaches: the fact that a serious attack on the organisation is a daily possibility. With this as the backdrop, we pose the fundamental question: do you really know who has access to your company's most important assets, and do you really trust them?

Trust is a prerequisite of business; it always has been. For markets and industries to function, there needs to be a high level of trust between businesses and their employees - whether temporary, permanent or contracted - as well as partners and suppliers.

However, managing and protecting information and access continues to be a thorny issue for many CIOs, who have to operate in an increasingly exposed and porous security environment. With technologies such as BYOD and the internet of things, businesses are actively enabling a growing number of people to access data from a wide variety of devices. This has created a greater number of attack vectors for cybercriminals, whilst making core business systems more vulnerable than ever before.

Nevertheless, the vast majority of CIOs are certain they are securing their organisations sufficiently, and have control of their access. You might be one of them.

In an exclusive CIO UK survey, 122 Senior IT Decision Makers in organisations with 500+ employees expressed great confidence in their organisations' security. Most of them (94%) told us they have an information security strategy in place, with just 5% of respondents feeling their organisation is not well protected against today's security threats.

However, the business headlines tell a different story. In 2014, there were high-profile data breaches in every major business sector including retail, finance, technology, communications, entertainment and health.

The big question is: if leading corporations can be breached - ones that you would expect to have the tightest security and access controls - are we really as secure as we believe? Furthermore, how can we be more secure whilst enabling, rather than not limiting the business?

Other questions we need to ask ourselves are: if organisations believe they are protected against cyber crime, which comes from within and the outside, then why are so many companies being hacked? What are organisations missing, and what controls are needed to have an impact on People, Process, and Technology?

Many large enterprises struggle to stay on top of access control, and to meet the stringent regulatory and industry compliance demands. It gives rise to a range of problems: employees might have access to information without needing approval; there could be many accounts still present without active owners; and users could be keeping hold of unnecessary access.

Constant personnel moves can pose other problems: there could be an influx of users after mergers and acquisitions, making access control a complex operation. Alternatively, it could be that internal and external moves are not

94%
have an information security strategy in place

CIO | KPMG | RSA

99%
agree that trust is important.

being managed effectively, leaving the organisation vulnerable to compromise from the inside.

This is the reality of business, and this is the security landscape in which we now operate. So, are we really as secure as we believe?

EMPLOYEE ACCESS MANAGEMENT AND TRUST

Trust is a cornerstone of corporate computing, and this is reflected in the survey results. The CIOs surveyed displayed high levels of confidence regarding their protection, with 95% saying they are adequately protected.

94% of UK organisations have an IS strategy in place, and 93% feel they are either very effective or effective at governing employees' access.

It is also clear that access management is high on the security agenda, with almost all the CIOs saying it will be on their agenda during the next 12 months.

On the surface, these results are excellent. They exude confidence, and paint a very encouraging picture of enterprise security today. But are things really that straightforward?

We suggest that there is a 'Trust Paradox' here. In other words, you need to trust your employees and business partners in order to get anything done. (99% of respondents agree that trust is important – or very important - when securing organisation assets, and very few said it was not very important.)

However, at the same time, 60% of respondents expect an attack to come from inside the organisation, with far fewer, 39%, saying a security breach would come from an external source.

Together, these results pose an interesting conundrum: trust is vitally important, but organisations don't necessarily trust their employees when it comes to security.

There are several reasons why this may be the prevailing perception. Firstly, CIOs and senior IT and security leaders need to display high levels of confidence, both in the organisation's security and its employees. They also need to convince business heads that the organisation is secure. Security and trust are a matter of perception as well as reality. We know from recent, high-profile security breaches that they can rock consumer confidence, as well as making employees uneasy, not to mention business partners and investors.

Secondly, media coverage tends to focus on big, external hacker attacks and not internal breaches. Perhaps this helps to play down the internal threat in peoples' minds. CIOs in the survey rightly identify the potential for an internal security breach, but other findings in the research suggest they are not being proactive enough in managing employee access.

Thirdly, there may be a false sense of security amongst UK organisations. Just because your company hasn't been hit yet, it doesn't prove you're secure: an attack is always imminent. Security analysts have noted an almost 100% increase in targeted internet-based attack campaigns between 2013 and 2014. Furthermore, internet security breaches rose by almost two thirds year on year, and a high proportion of major web sites have been found to contain critical vulnerabilities.

60%
expect an attack from inside the organisation.

"Wherever the threat comes from, information and IP is arguably the most important asset within an organisation. At a base level, the IP thefts are following some form of exploitation of trust, so reducing the footprint of trust reduces the likelihood of theft."

Matt White, Senior Manager at KPMG in the UK

Regarding the internal threat, consider this common scenario: a company hires a contractor for a three-month project, with HR and IT departments involved. They need to give them access to information, and work with the hiring manager to review their access. So far, so good. But what happens when the contractor leaves? Who updates their access? What audit controls are in place? For many, this can be a point of weakness in the organisation.

For situations like these, tools are available to mitigate risk. Malcolm Marshall, KPMG's global head of cyber security, says, "These solutions are often seen as blockers to a company, restricting access and making it harder to do a job, but, by combining software such as RSA IMG with consultancy services to enhance people and process changes, you can affect increased security with improved efficiency and transparency."

"With this in mind, KPMG work closely with RSA to provide an offering that drives the business forward, whilst reducing the risk of uncontrolled access. The effect is a justifiable confidence in the systems in place, which whilst not infallible will reduce the risk and decrease the required level of trust."

100%
increase in targeted internet-based attack campaigns

Another area of the survey that prompted questions is around how frequently organisations review their employee's level of access. A third of respondents said they did this annually, 14% bi-annually, and just under a third quarterly. Surprisingly, 16% review their access less frequently, with some of them not reviewing access at all.

It may be worth asking: is it really enough to review employee access so infrequently? A lot can happen in a year! Are we at risk of being more reactive than proactive?

Surely if CIOs are expecting the attack to come from within, then they need to continually, or at least more regularly review things like levels of access?

The survey also revealed a lack of expectation of a threat from competitors, with just 2% saying that if they were to have a security breach, the most likely source would be the competition.

In reality, IP theft is a hidden and unreported crime. Estimates have put the cost of IP theft from US corporations at around £200bn per year, with a large proportion of the attacks coming from China.

REGULATION AND COMPLIANCE

Controlling employee access and achieving governance has grown more complicated over time, due to the diverse mix of applications and access scenarios that have developed to date. Consequently, identity and access management can be extremely complex and time-consuming for IT leaders and their teams.

Although some companies may have implemented comprehensive and agile tools to control user identity and access, and thereby manage their internal risk effectively, many do not. Access management remains patchy for many companies, with a lack of linkage between access controls and governance polices.

Access management and auditing is also a costly affair for many organisations: both financially and in terms of hours, because it can be a heavily manual process.

Consider your own organisation. Do you have a clear path to governance, with unified, enterprise-wide, and policy-based visibility and control?

Are your access management processes sufficiently dynamic, and do they cover applications, unstructured data, privileged accounts, and access to information by contract and temporary staff as well as permanent employees?

According to our survey, 83% of CIOs said they can prove to the regulators or auditors they are in control of their employees' access (11% weren't sure and 6% said they could not).

Interestingly, 27% said an audit finding would trigger a review of their employees' level of access, with over a fifth saying they would carry one out on the back of a regulator request or

inquiry. 20% said adoption of new technology would lead them to review access levels, and the same proportion would do it after mergers and acquisition activity.
Considering the high risk of an insider threat to the organisation, is it sufficient to be this reactive, rather than proactive in monitoring and reviewing employees' level of access?

We suspect that the financial and time costs of auditing access control and management can be very high for most organisations, keeping in mind that many of the respondents only review their employees' level of access annually (32%) or quarterly (29%).

White says, "Reporting for auditors and regulators often requires the collating of multiple information sources, usually across many departments and geographies. Frequently a manual process, requiring input from a number senior employees, the end to end process is both time consuming and costly."

"Once more by combining process improvement with technology you can increase efficiency and reduce staff overhead. KPMG Access Manager brings together industry leading technology from RSA and the award winning consultancy from KPMG to simplify the management of access and subsequently streamline the reporting for auditors and regulators."

So, what does it cost your organisation to provide information to audit or regulatory authorities? In addition, do you have controls in place today that allow you to support a dynamic environment: one that puts you in charge of employee access and means you can proactively combat attacks from inside or outside the enterprise?

If the answer is that the financial and time costs are higher than they should be, or the security environment is not sufficiently dynamic, automated or integrated, then perhaps it's time for a change.

CONCLUSION

Almost all the CIOs we surveyed said they think trust is important in securing their assets. They felt their business was adequately or very well protected, but if there were a security breach, the most likely source would be inside the organisation.

Regardless, a fifth of respondents are not confident their employees have the right level of access to assets, and the majority chooses to review levels of access annually or twice a year, rather than continually. This points to a Trust Paradox: people are, as is often the case, the weakest link in the chain. Perhaps we need to focus more closely on the trusted relationship between the organisation and its people, rather than relying on blind trust and false confidence in current IS systems and strategies.

There is clearly room for improvement, and eight in 10 senior IT decision-makers we asked seem to be aware of this: putting access management on their agenda over the next 12 months.

The Trust Paradox needs to be mitigated rather than eliminated with the right blend of trust, processes and technology.

Enterprises can become more secure if they implement Processes that are more proactive, ongoing and analytical, and Technologies that feature automated, end-to-end, integrated security. These tools and methodologies are available today to mitigate the business risks outlined in this paper. By improving employee access management and security, you can raise trust levels across the organisation.

Moreover, by putting the right tools and methodologies into place, you will be able to change culture in your organisation to keep up with advances in technology and the changing nature of the workforce, as you continue to digitise your operations.

This whitepaper is brought to you by CIO UK in association with KPMG and RSA.

CIO | KPMG | RSA