Close the password security gap: convenience for employees and control for IT

Employee education isn’t the only answer to password management
SUMMARY

CATALYST

Companies know they have problems with password security, yet they are not taking steps to remedy the issues. Indeed, far too many of them rely entirely on their employees to manage their passwords, with no technology in place to enforce password strength or the frequency of password refresh, even though they are aware that employees are the weakest link in the chain.

Ovum surveyed IT executives at enterprises across North America, Europe, and Asia-Pacific about password management to determine how they are approaching the challenges of granting and controlling employee access, both to enterprise applications on company premises and to sanctioned cloud-based ones. We also spoke to corporate employees across the same geographies to ascertain how they view the question of managing the passwords they need to do their jobs. We focused on password facilities in place, including strength and frequency, as well as how those are enforced.

Our objective was to understand how employees approach passwords and what companies are doing to address those habits and password security overall.

OVUM VIEW

The picture that emerges from Ovum’s twin surveys of corporate employees and IT executives with responsibility for security gives us cause for concern. In many cases, password management practices remain stuck in a bygone era, overly reliant on manual processes and, far too often, placing an excessive level of trust in employees’ awareness of their duty to “do the right thing.” While we applaud efforts to instruct staff members on good password practices and to maintain their awareness, the absence of technology to underpin policy is widespread, leaving companies unnecessarily at risk from weak or shared passwords, not to mention ones that have been in use for too long.

KEY MESSAGES

• Employers know they have a problem and are still not doing something about it.

• Almost half of employees admit that passwords have an impact on their productivity.

• Lack of control over cloud apps is widespread.

• Manual password security and policies are extremely common.

• Too many organizations leave password security in their employees’ hands.

• Most employees would use a password manager if their company offered one.
LACK OF CONTROL IS A PROBLEM FOR MOST COMPANIES

OVER 75% OF COMPANIES LACK COMPLETE CONTROL OF SAAS APPS USED BY THEIR EMPLOYEES

FIGURE 1
OF THE CLOUD-BASED APPLICATIONS YOU ARE AWARE OF, WHAT PERCENTAGE DOES YOUR IT TEAM NOT MANAGE AND CONTROL IN REGARDS TO ACCESS, PROVISIONING, ETC.?

Source: Ovum

A key finding from our study is that full control by the IT department of the software-as-a-service (SaaS) cloud applications used in an organization is far from the norm. Seventy-eight percent of respondents in the IT exec survey said they did not have control of all the cloud-based applications the company’s employees were using, with 25% saying they believed they were controlling less than half.

IT KNOWS THIS IS A PROBLEM BUT ISN’T MOVING TO ADDRESS IT

On the plus side, IT executive respondents are well aware of the challenge inherent in this lack of control: 68% of them saw significant or very significant risk from the gap in control over what applications their organizations’ employees are using. However, that awareness does not translate into action to remedy the situation.
WEAK PASSWORD SYSTEMS PUT USERS AND BUSINESSES AT RISK

EMPLOYEES ARE BEING LET DOWN BY THE VERY SYSTEMS THAT ARE SUPPOSED TO BE KEEPING THEM SAFE

FIGURE 2
EMPLOYEES IDENTIFIED A MULTITUDE OF PASSWORD MANAGEMENT PROBLEMS

- I am obliged to change my passwords on a regular basis: 18%, 16%, 10%
- Not all applications are single sign-on, so I need multiple passwords as a result: 17%, 28%, 11%
- I struggle to come up with passwords that are strong enough to meet the system’s criteria on a regular basis: 16%, 10%, 19%
- I don’t have anywhere I can securely store all my passwords: 14%, 7%, 12%
- I can’t remember all of my passwords, so I have to reset them frequently: 13%, 12%, 17%
- Each password has to be complicated and long: 13%, 10%, 24%
- Policies require me to have multiple passwords for different apps/sites: 9%, 17%, 8%

Source: Ovum

Ovum: Research and thought leadership
Employees have multiple problems managing passwords and are not getting the help they need. More than three-quarters of employees reported that they regularly have problems with password usage or management. Most confirmed they are dissatisfied with weak password systems that don’t provide the support they need.

Major pain points include regularly having to change passwords without the levels of support needed to make this a simple, safe, and automated process, all of which can have a significant impact on employee productivity – 44% of respondents said this is a major issue. Because employees are being left to fend for themselves, problems extend into associated areas; therefore, simply coming up with strong enough passwords to fulfill company requirements also becomes a serious issue. Password usage problems are exacerbated by the lack of single sign-on (SSO) in many organizations. Fifty-six percent of the organizations we surveyed did not have SSO available, which, for many users, means that every required password change must be dealt with on an individual basis.

THE ABSENCE OF EFFECTIVE SSO IS A SIGNIFICANT WEAKNESS

Employees struggle to manage and maintain the ever growing number of passwords they need to use each day. As highlighted earlier, many of the problems are caused by a lack of key password management facilities and a reliance on manual processes. The situation is complicated by the lack of SSO facilities that can be used alongside password management systems to smooth and cut down on the number of individual access requests required as users move between their various business systems. Employees said problems arise directly from the use of multiple passwords. Therefore, as some 60% of respondents don’t have access to SSO facilities, and a further 22% have only partial SSO, more than 80% of users are at risk.
COMPANIES KNOW SAAS APP ACCESS IS A PROBLEM

SAAS AND CLOUD APPS ADD TO THE OVERALL PROTECTION AND CONTROL REQUIREMENTS

The use of SaaS and cloud-based systems by employees is linked to their operational roles within the business and adds to the number of operational systems and unique passwords that need to be managed. Our research shows that, on average, more than 50% of respondents must use a new or unique password for each business system they need to access. This applies to on-premises and cloud-based applications and systems and has a direct overhead that is linked to the number of systems in use. Hence, as the number of physical and cloud-based systems increases, so does the need to move away from the use of ineffective and manual password control systems.

THERE IS LACK OF VISIBILITY INTO SAAS APPLICATIONS IN USE

FIGURE 3
HOW CONFIDENT ARE YOU THAT YOU KNOW ALL THE CLOUD-BASED APPLICATIONS YOUR EMPLOYEES USE TO COMPLETE THEIR WORK?

Source: Ovum

The problem of controlling access begins with the lack of visibility afforded by SaaS applications. Twenty-seven percent of IT execs described themselves as “not sure,” “not confident,” or “really not confident” about the number of SaaS applications employees use. You cannot control what you don’t even know about. This is the problem of “shadow IT.” Employees find SaaS applications for use at home, then bring them into the workplace to do their jobs, without consulting or even notifying the IT department.
We asked IT execs what they were doing to enforce strong passwords and were surprised to find that 61% of them rely exclusively on employee education. In other words, they instruct their employees on how to create their passwords using numbers, letters, and characters, as well as how to change them, but do not enforce these behaviors.

It was encouraging to hear from 24% of IT execs that they already have a password manager in place, and that an additional 8% of them were planning to install one over the next year. However, 37% told Ovum that they still rely on entirely manual processes to manage user passwords for cloud applications.

For the process of changing passwords, almost three out of 10 execs (29%) said they rely on manual processes, with no system messages to warn users of the impending need to change. Alarmingly, a further 7% said their company does not require password refreshes at all (i.e., once set up, they never change them).

**Source:** Ovum

We asked IT execs what they were doing to enforce strong passwords and were surprised to find that 61% of them rely exclusively on employee education. In other words, they instruct their employees on how to create their passwords using numbers, letters, and characters, as well as how to change them, but do not enforce these behaviors.

From there, the employees are on their own, with no technology in place to enforce any password strength requirement. This means that if individual employees decide to jettison all that they have learned and go for some other kind of password without any of the requisite mix of numbers and letters, or upper- and lowercases, there is nothing to stop them.
DEFENSE AGAINST PASSWORD SHARING IS FAR TOO WEAK

IT EXECS RANKED PASSWORD SHARING AS HIGH RISK

Thirty-seven percent of respondents to our IT exec survey ranked password sharing on paper as “high risk,” and 34% put sharing via email in the same category. Now, Ovum recognizes that some level of password sharing may be necessary in certain enterprise departments and, of course, must be done securely where that is the case. Nonetheless, when asked how they guard against password sharing in scenarios where it is an avoidable risk, 44% of companies said they engage in ongoing employee education programs, and 20% said they ban it contractually, making it clear to employees that it is banned when they join.

Respondents to this question could choose only one option, so we can conclude that 64% of them have no technology in place to avoid unnecessary password sharing. Twenty-two percent said they monitor password and user activity to detect password misuse, and only 14% said they have automated control facilities in place.
FIGURE 6
DO YOU EVER SHARE PASSWORDS WITH YOUR CO-WORKERS?

![Figure showing the percentage of employees who share passwords]

Source: Ovum

There is widespread recognition on the part of IT execs that, barring special situations in which sharing passwords with co-workers or other third parties is necessary, the practice is, by definition, a bad one and should be discouraged. Nonetheless, far too many employees are prepared to do this.

Eleven percent of employees are prepared to share passwords with co-workers from inside the business, and, of even greater concern, nearly half as many (5%) have shared passwords with someone from outside their organization. At 11%, the internal password sharing response remains too high. In effect, it means someone in virtually every organization surveyed is potentially putting systems access credentials, and with them their business systems, at risk.
THE PASSWORD SHARING PROBLEM IS A MAJOR ISSUE FOR BUSINESSES

The password sharing problem multiplies for medium to large business organizations, so that on average, in a 5,000-user organization, there is the potential for around 550 employees to be sharing their systems access credentials. Therefore, unless a password management tool that includes user monitoring and usage controls is in place, there is nothing to stop this from happening.

Eleven percent sharing passwords with co-workers is the headline number and the average across all areas we surveyed. However, because we have undertaken a wide-ranging global investigation, we had an opportunity to look at countries where password sharing appears to be out of control. At 22%, Australia and Hong Kong were the countries where most employees were prepared to share credentials with co-workers. At the other end of the scale, German employees were the least likely to share their password credentials with co-workers.

ENTERPRISES ARE EXTREMELY VULNERABLE WHEN PASSWORDS ARE SHARED WITH OUTSIDERS

The percentage of employees who have shared passwords with someone outside their company may be lower at 5%, but because of the heightened risks involved, this is 5% too many. Using the enterprise example once again, on average, in a 5,000-user organization, around 250 employees are likely to be sharing their business access credentials with an outsider.

The key issue is that it takes the misuse of only one shared or stolen credential to put an organization and its business systems at risk.

“... IN A 5,000-USER ORGANIZATION, THERE IS THE POTENTIAL FOR AROUND 550 EMPLOYEES TO BE SHARING THEIR SYSTEMS ACCESS CREDENTIALS.”
The take-up of social credentials by employees to access business systems is a growing issue. It needs to be properly addressed, rather than simply being tolerated, as appears to be happening. Our research shows that 23% of employees are using social media credentials to sign in to business systems and applications. The 25% approval rating shown in Figure 7 also confirms that business organizations are keeping pace by offering sanctioned use of social credentials, and therefore most users who are doing this have the right permissions.

What this apparently harmonious position doesn’t highlight very well is that very few extra security controls have been added to help monitor and control the right levels of social usage and ensure that when access to sensitive information is required, higher forms of authentication can be requested. If employers are going to rely on employees’ personal accounts as secure logins to their organizations, they also need to ensure that those accounts are secure. Those that approve the use of social credentials must also take responsibility for managing those credentials and where necessary provide multifactor authentication controls.

### APPROVED USE OF SOCIAL CREDENTIALS IS ON THE RISE AND REQUIRES ADDITIONAL CONTROLS

**FIGURE 7**

**COMPARING USE OF SOCIAL CREDENTIALS**

<table>
<thead>
<tr>
<th></th>
<th>NO (77%)</th>
<th>YES (23%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you use your social media credentials to sign in to business apps?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you allowed or encouraged to use your social media credentials to sign into business applications?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Ovum
LACK OF CONTROL PUTS EXCESSIVE RELIANCE ON END USERS

It is Ovum’s opinion that the previous sections demonstrate an inherent weakness in many companies’ password management. Whether it be how they guarantee the strength of the passwords in use, the overly manual approach taken to changing passwords, or what controls they have in place to avoid password sharing, the data we have collected reveals an unacceptably insecure scenario.

Employee education is, of course, a good thing and should be carried out with refresher courses at regular intervals to keep staff up to date with a company’s security posture and practices. It should not be thought of as a panacea for password security, however, and must be backed up with the appropriate technology.

MOST BUSINESSES HAVE DEFINED PASSWORD USAGE POLICIES BUT DON’T HAVE THE ENFORCEMENT SYSTEMS TO BACK THEM UP

Close to 80% of employees said password policies are in place for lockout, complexity, change management, and education and training issues. They were less clear when it came to issues around frequency of change and what would happen if the rules were not followed. Employees confirmed that usage policies are in place, but there is relatively little control when it comes to the required levels of enforcement.

These are important differentiations because, without the right combination of usage policies, education, and technology-based enforcement, too much emphasis and too much responsibility are being placed on individual employees to do the right things. Failure by users to do the right thing every time they attempt to access business systems can put both themselves and the business at risk. It can result in accidental or intentional damage and/or data loss, but without the password management and monitoring systems needed to manage each access and usage request, business organizations are not in a strong position to identify and respond to the actions of their employees when something goes wrong.
Sixty-four percent of employees said they experience regular, at least once per month, password usage problems. A further 12% said these types of problems occur more frequently. There does seem to be a lot of self-help going on, but this may have been due to shortfalls in available support systems and still left more than a third of users (36%) needing help desk support at least once every month.

Our investigations identified a general lack of awareness from employees about the benefits a password management system would provide for everyday users.

Nevertheless, when the benefits were explained and if a tool was offered that would help store and access passwords without needing to remember each one, 69% of respondents said they would want to use it. Most also agreed there were benefits to be gained from deploying a password management system. Employees and everyday users are being put at risk; too much responsibility is being placed on them to keep insecure and weak password systems safe, and insufficient controls are in place to stop unsafe activities from happening.
RECOMMENDATIONS

RECOMMENDATIONS FOR ENTERPRISES

IT KNOWS THERE IS A PROBLEM, SO FIX IT

Our survey of IT executives showed clearly that most companies are aware there is a problem of lack of visibility and control with regard to employees’ access to software-as-a-service applications, yet in the majority of cases they are not doing enough, and many are not doing anything, to address the situation. The availability of SaaS apps is only going to increase, and the potential for a Wild West situation of uncontrolled use of dozens of such apps by corporate employees is only going to grow, so it is time to do something, if not to rein in, then at least to assert greater control over this situation.

USE TECHNOLOGY TO UNDERPIN PASSWORD SECURITY INITIATIVES

Employee education is never to be decried and should form the basis of all security activities in companies of all sizes. An educated workforce is an empowered one, and the “I didn’t know that was a security risk” scenario all too often reveals the weakest link in any infrastructure.

That said, exclusive reliance on your employees to do the right thing represents, in Ovum’s opinion, an excessive degree of trust. What happens when employees, however well-trained on matters of password security they may be, need to get something done quickly, and the easiest way is to share a password with someone else, within or outside the organization? The need to be productive may outweigh their concern for security on that occasion, and that may be the fatal moment.

Similarly, unless password strength is obligatory, the temptation to go for something more easily remembered may be too great, particularly if employees are accessing a lot of applications, each with a different password.

Therefore, Ovum recommends the deployment of technology to underpin password security, forcing compliance with password strength as well as alerting employees that they will need to change their passwords in the next few days and so on.

INTRODUCE PASSWORD MANAGEMENT TO HELP EMPLOYEES AND IMPROVE SECURITY

Our survey of employees found them to be generally in favor of using password management technology in the workplace, and employers should facilitate this. Employers should also recognize that most employees would welcome help from a password manager, making it an easy win for such technology to be introduced. It should be positioned as a means of helping staff members remember all the different passwords they use.
METHODOLOGY
Ovum surveyed 355 IT executives and 550 corporate employees, covering 13 vertical markets in the three major business regions of the world (North America, Europe, and Asia-Pacific). The survey included questions on password management procedures in their respective organizations, both in terms of how things are done today and what benefits or obstacles they envisage regarding the implementation of password manager technology.

AUTHOR
Andrew Kellett
Principal Analyst, Infrastructure Solutions
andrew.kellett@ovum.com

Rik Turner
Principal Analyst, Infrastructure Solutions
rik.turner@ovum.com

OVUM CONSULTING
We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com