"Putting paid to password pain"

The Australian 31/10/06.

CASE STUDY **WESTERN AUSTRALIAN INDUSTRIAL RELATIONS COMMISSION**

The days of complex double logins are over, **Andrew Colley** reports

WHEN Western Australia's industrial relations umpire began letting its commissioners and staff access documents on the road two years ago, it knew the days of its static password system were numbered.

Mysterious double logins and password-under-the-keyboard syndrome rankled security auditors and help-desk jockeys.

There was increasing concern that documents containing allegations of workplace sexual harassment or details of sensitive industrial negotiations could appear before the wrong eyes.

"A limiting factor for us was when we started to allow remote access to our network for some key users," chief information officer Andrew Waddell says.

"We discovered there were some instances of these users remaining logged on remotely when they were also logged on here at the office, and there was no way they could have been logged on in both places at once."

The commission installed RSA's SecurID two-factor authentication self-destroying password system at the gate of its virtual private network, for less than $10,000, including the cost of deploying 75 tags at about $70 for each user, and a new authentication server.

RSA's two-factor security system requires staff to enter a user login, a PIN and a self-destroying numeric password generated by a digital security token.

The token is synchronised with the commission's authentication server to produce valid passwords every 60 seconds. Without all three identifiers, including the temporary numeric password, the system rejects login attempts.

After ironing out some bugs in early versions of the RSA software and getting over a few user education problems, the system eradicated human security hazards that proliferated under the old pass phrase system. Calls to the help desk became more frequent as commission staff struggled with security directives to use more complex passwords and to change them more frequently.

"The more complicated you make a password the harder it is for someone to remember," Waddell says.

"And the more often it is changed, the more likely the user is to only make a small change.

"The bottom line is that the more we tried to enforce passwords the more likely someone was to write the thing down on a sticky note and put it under their keyboard."

Since the system has been in use, password-related calls to the commission's help desk have dwindled from one or two a week, to one a month.

"It has reduced our help desk costs," he says,

The commission has now begun experimenting with software that will let smartphones, including BlackBerry devices and iMate mobile phones, generate the numeric pass codes in place of security tokens.

THE PROBLEM

A static password system was becoming frustrating for staff and inadequate to handle an increase in remote logins.

THE PROCESS

Two-factor authentication tokens were introduced. They generate self-destroying passwords to tighten and simplify login security.

THE RESULT

Security is tighter and help desk costs are down in line with a drop in password-related support calls.

"Putting paid to password pain"

The Australian 31/10/06

CASE STUDY **WESTERN AUSTRALIAN INDUSTRIAL RELATIONS COMMISSION**

The days of complex double logins are over, **Andrew Colley** reports

WHEN Western Australia's industrial relations umpire began letting its commissioners and staff access documents on the road two years ago, it knew the days of its static password system were numbered.

Mysterious double logins and password-under-the-keyboard syndrome rankled security auditors and help-desk jockeys.

There was increasing concern that documents containing allegations of workplace sexual harassment or details of sensitive industrial negotiations could appear before the wrong eyes.

"A limiting factor for us was when we started to allow remote access to our network for some key users," chief information officer Andrew Waddell says.

"We discovered there were some instances of these users remaining logged on remotely when they were also logged on here at the office, and there was no way they could have been logged on in both places at once."

The commission installed RSA's SecurID two-factor authentication self-destroying password system at the gate of its virtual private network, for less than $10,000, including the cost of deploying 75 tags at about $70 for each user, and a new authentication server.

RSA's two-factor security system requires staff to enter a user login, a PIN and a self-destroying numeric password generated by a digital security token.

The token is synchronised with the commission's authentication server to produce valid passwords every 60 seconds. Without all three identifiers, including the temporary numeric password, the system rejects login attempts.

After ironing out some bugs in early versions of the RSA software and getting over a few user education problems, the system eradicated human security hazards that proliferated under the old pass phrase system. Calls to the help desk became more frequent as commission staff struggled with security directives to use more complex passwords and to change them more frequently.

"The more complicated you make a password the harder it is for someone to remember," Waddell says.

"And the more often it is changed, the more likely the user is to only make a small change.

"The bottom line is that the more we tried to enforce passwords the more likely someone was to write the thing down on a sticky note and put it under their keyboard."

Since the system has been in use, password-related calls to the commission's help desk have dwindled from one or two a week, to one a month.

"It has reduced our help desk costs," he says,

The commission has now begun experimenting with software that will let smartphones, including BlackBerry devices and iMate mobile phones, generate the numeric pass codes in place of security tokens.

THE PROBLEM

A static password system was becoming frustrating for staff and inadequate to handle an increase in remote logins.

THE PROCESS

Two-factor authentication tokens were introduced. They generate self-destroying passwords to tighten and simplify login security.

THE RESULT

Security is tighter and help desk costs are down in line with a drop in password-related support calls.