Executive Summary

In 2014 Lieberman Software surveyed nearly 280 IT security professionals at RSA Conference 2014 in San Francisco, CA. The survey measured attendees’ insights into password security, cloud security, and other current hot button cyber security issues.

RSA Conference was selected as the venue for the survey due to the demographics of its attendees. According to the event’s web site, this show “has consistently attracted the world’s best and brightest in the field, creating opportunities for conference attendees to learn about IT security’s most important issues through first-hand interactions with peers, luminaries and emerging and established companies.”

The following sections summarize the survey results. Highlights include:

- More than 13% can still access a previous employers’ systems using their old credentials.
- More than 20% do not have, or don't know if they have, a policy to ensure that former employers and contractors can no longer access systems.
- Almost 25% work in organizations that do not change their service and process account passwords within 90 days.
- Nearly 80% choose to keep their organization's most sensitive data on their own network, rather than the cloud.
- Nearly 75% think the cloud applications their users download cause security headaches.
Access to Previous Employers’ Systems

Can you still access any of your previous employers’ systems using your old credentials?

- Yes: 13%
- No: 79%
- Other: 8%

If yes, how far back can you still gain access?

- Previous Employer: 61%
- Previous Two Employers: 23%
- All Previous Employers: 16%

Former IT employees and contractors are potentially serious security threats to an organization. They generally have the password secrets that allow them to login to systems and applications throughout the network. If their former privileged logins are not shut off, odds are these ex-employees can still gain access even long after their employment ends.
Policies to Prevent Former Employer Access

Does your company have a policy to make sure contractors cannot access your systems once they leave?

Fortunately, most survey respondents do work for organizations that have a policy to prevent former employees from gaining access after leaving. Those who do not should beware the case of Jason Cornish - a former employee of pharmaceutical company Shionogi, who was able to destroy most of the company's computer infrastructure after being laid off.
Frequency of Service Password Change

How often do you change service and process account passwords within your organization?

- Daily: 2%
- Monthly: 22%
- Quarterly: 53%
- Twice a year: 9%
- Annually: 6%
- Never: 8%

If never, do you choose not to change a service or process account password because it could potentially cause outages and downtime?

- Yes: 50%
- No: 45%
- Don’t Know: 5%

Service and process account passwords are privileged logins that can be stored in services, tasks, COM applications, IIS, SharePoint, databases, and applications. Service and process accounts are incredibly difficult to change manually because first you have to identify everywhere the service account is in use, and then you must change the password in all of those places. As a result, some organizations simply ignore the problem.
Cloud vs. On Premises

Do you choose to keep your more sensitive data on your organization's own network rather than the cloud?

IT professionals are aware there is limited data privacy in cloud environments and therefore it is not a surprise that many prefer to keep their most sensitive assets on premises. What is interesting though, is that when Lieberman Software asked this same question in November, 2012, 86 percent of respondents said preferred to keep sensitive data within their own network, rather than the cloud. This essentially means that trust in the security of the cloud has increased over the last year, despite the impact of the NSA scandal.
Government Surveillance and the Cloud

Thinking about your organization, does the thought of government snooping deter you from keeping data in the cloud?

IT professionals generally realize that if a government or official body wants to see what data a company is holding, the cloud host involved is legally obliged to provide them access. As a result, many IT pros might think twice about migrating to the cloud. Interestingly, when Lieberman Software asked this same question in November, 2012, 48 percent of respondents were discouraged from using the cloud because of fear of government snooping. It would appear that trust in the cloud is increasing.
Security of Cloud Applications

Do you agree that the cloud applications that your users download cause security headaches?

Users who run with elevated privileges can introduce all sorts of IT headaches by downloading and installing applications, and changing their system configuration settings. An organization would be wise to strictly control and monitor the privileged actions of its users.
Size of Organization

What is the size of the organization you work for?

- More than 5,000 people: 38%
- 1,011 – 5,000 people: 16%
- 501 – 1,000 people: 7%
- 101 – 500 people: 15%
- Less than 100 people: 24%
Survey Methodology

The 2014 Survey of IT Security Professionals was conducted among 278 attendees of RSA Conference 2014 in San Francisco. All responses were anonymous.Respondents were all registered attendees of the show and were polled one on one, on site at the venue. Only fully completed surveys were measured for this report. Any incomplete responses were discarded by the tabulators.

Limitations

The number of surveys was dependent on time constraints. Lieberman Software conducted as many surveys as possible during the allotted time while attendees were present on the show floor. Surveys were continually conducted, in person, until the exhibit hours ended.

About Lieberman Software

Lieberman Software provides privileged identity management products to more than 1200 enterprise customers worldwide, including nearly half of the Fortune 50. By automatically locating, securing and continuously auditing privileged accounts, both on-premises and in the cloud, Lieberman Software helps protect access to systems with sensitive data, thereby reducing internal and external security vulnerabilities, improving IT productivity and helping ensure regulatory compliance. The company developed the first solution for the privileged identity management space, and its products, including Enterprise Random Password Manager™, continue to lead the market. Lieberman Software also provides a mature line of Windows security management tools. The company is headquartered in Los Angeles, CA, with offices and channel partners located around the world. For more information, visit www.liebsoft.com.