LIEBERMANSOFTWARE™

RSA Conference Survey

March 2016

Executive Summary

In March, 2016 Lieberman Software Corporation surveyed IT security professionals at RSA Conference 2016 in San Francisco, CA. The survey focused on attendees' opinions toward the current state of cyber security, including the viability of passwords as a verification method and the likelihood of attendees' existing IT security products preventing a cyber attack on their organizations.

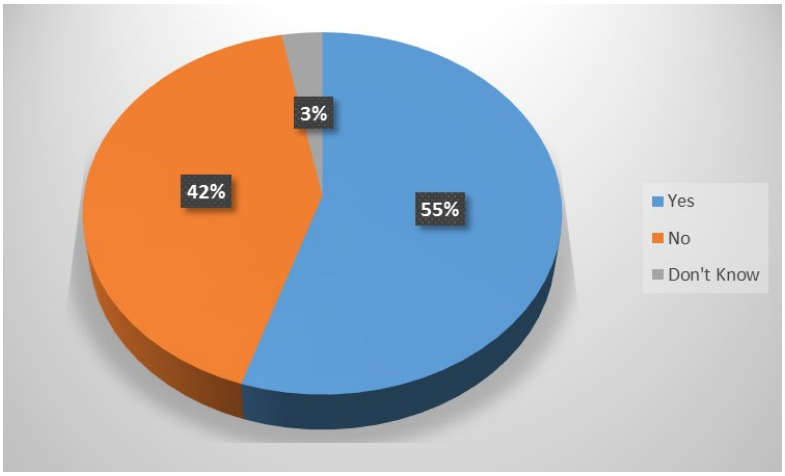
The survey was conducted at RSA Conference due to the demographics of its attendees — more than 40,000 IT security professionals who attend the show from all regions of the world and all major vertical markets.
This report summarize the survey results, broken down by each question. Survey highlights include:

- 55% of respondents make users change their passwords more regularly than they change the administrative credentials.
- 10% of those surveyed never change their administrative credentials.
- 53% of respondents say that modern hacking tools could easily break passwords within their organizations.
- 77% think that passwords are failing as an IT security method.
- 36% work in organizations where IT staff share the same password.
- 45% said their organization is not prepared to defend against a cyber attack, despite the IT security technology they've deployed.

1. Do as We Say, Not as We Do

Changing user passwords has long been a basic – and well known - tenet of IT security. But when it comes to password security, privileged passwords (admin, root and the like) are often overlooked. As we discovered in this survey, most organizations make their users change passwords more often than the administrative credentials are updated.

Would you agree with this statement – We make our users change their passwords more regularly than we change the administrative credentials?



Without an automated solution to discover, track and update all the privileged credentials that exist in large networks, administrative passwords are rarely updated. But because of the systems with sensitive data that these credentials protect, frequent privileged password updates are essential.

However, as the results of the next question show, this practice is rarely performed.

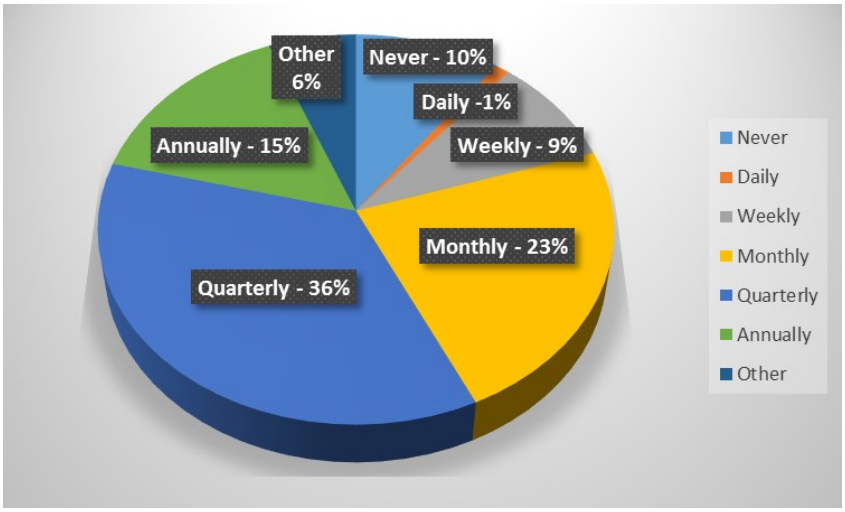
2. Slow to Change

Changing user passwords has long been a basic – and well known - tenet of IT security. But when it comes to password security, privileged passwords (admin, root and the like) are often overlooked. As we discovered in the previ-

ous question on this survey, most organizations make their users change passwords more often than the administrative credentials are updated.

Most major regulatory compliance regulations require organizations to change privileged credentials at least every 30 days. Only 33% of respondents to the survey have a password frequency rate of 30 days or less. Even a 30 day password update rate may not be frequent enough. Cyber intruders and malicious insiders are looking for passwords that let them jump from system to system on a network until they find what they want. And 30 days is a long time for them to exploit stolen privileged credentials until they're invalidated. Only 1% of those we surveyed are changing their administrative passwords daily.

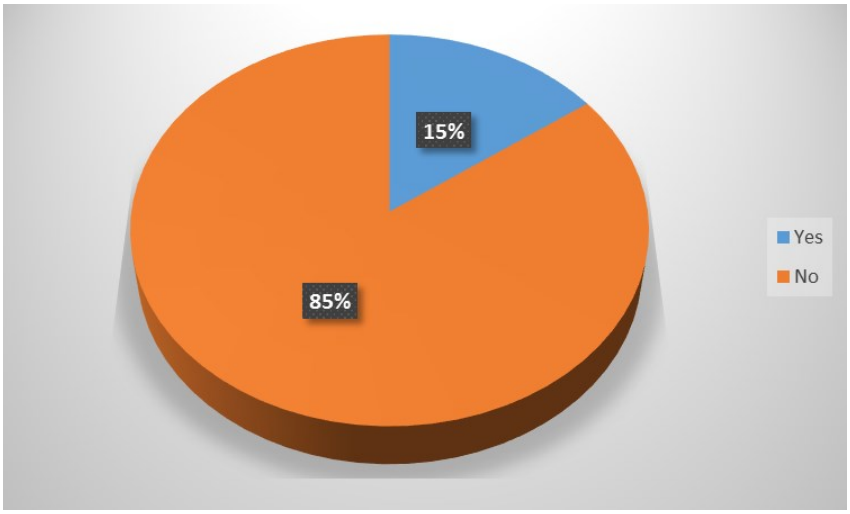
How often do you change your administrative credentials?



3. Gone But Not Forgotten

Former IT employees and contractors are potentially serious security threats to an organization. They often know the password secrets that let them login to systems and applications throughout the network. If privileged credentials aren't continuously changed, essentially shutting off former employee's privileged logins, odds are these ex-employees can still gain administrative access even long after their employment ends. It should be alarming that nearly one in six survey respondents are confident that they could still login with their administrative credentials if they left their organizations.

If you left your organization could you still access the admin credentials remotely?

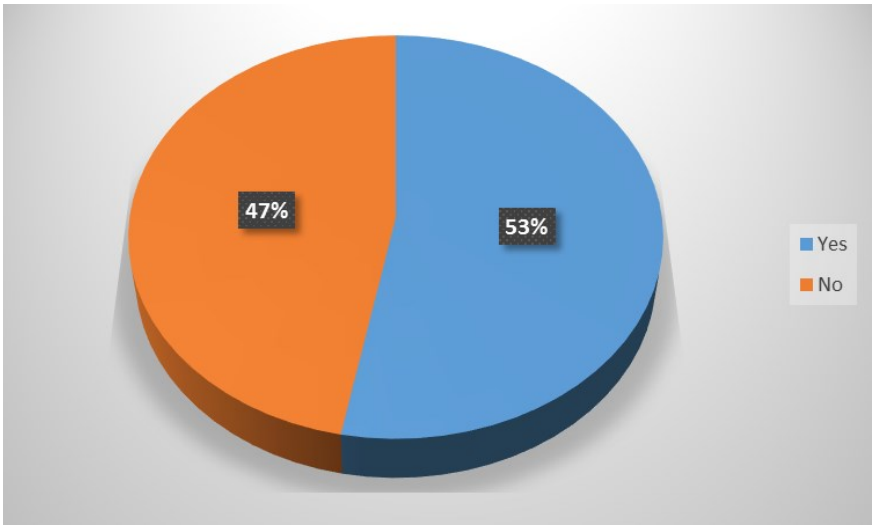


4. Picking the Locks

The majority of survey respondents think that modern hacking tools could easily break their passwords. Rainbow tables and other tools are used by hackers to crack passwords and gain access to places they shouldn't be. Depending on the method used to crack a password, the password's age and length are relevant factors. If you're dealing with a brute force attack, then time is really what you're up against. The less frequently a password changes, the longer the window of time is for a hacker to obtain the password. Similarly, longer passwords have exponentially more character variations and therefore require more time to crack.

What this really means is that given the will to break into a computer, often all you really need is time. But by continuously changing the passwords for privileged accounts, you're denying your adversaries the time they need to succeed.

Do you think modern hacking tools could easily break passwords within your organization?

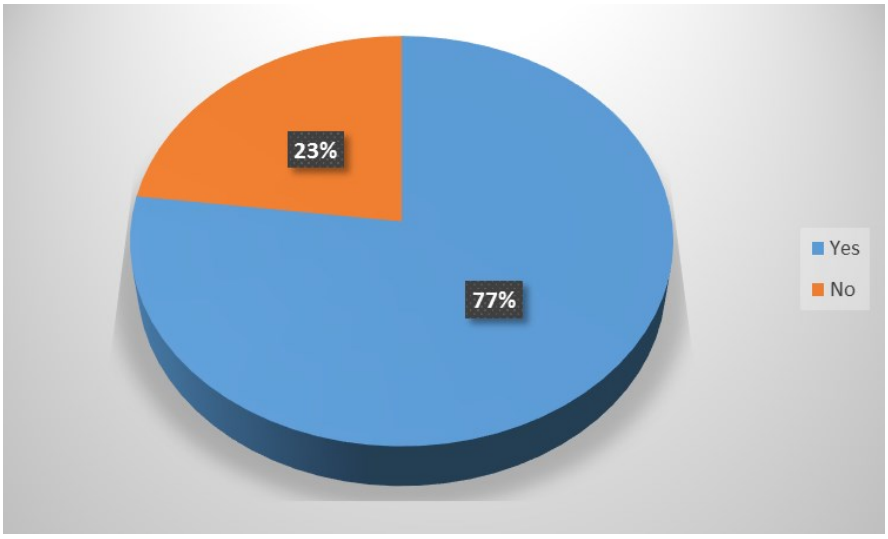


5. Password Fail

More than three quarters of survey respondents think that passwords are failing as an IT security method. Considering other findings in the survey – the lack of frequent credentials changes, the ability to login after leaving an organization and the ease with which passwords can be cracked – this overwhelming figure is not surprising.

Perhaps it's time to rethink how passwords are being utilized. Attackers use automated methods to steal credentials and gain privileged access to networks. To counter this threat, organizations should take this automated approach and apply it to their privileged credentials. Changing credentials continuously – with unique and complex values for each account - would go a long way toward keeping hackers from gaining unrestricted privileged access. And every time a human uses a privileged account - and the system will support it - multi-factor authentication should be used.

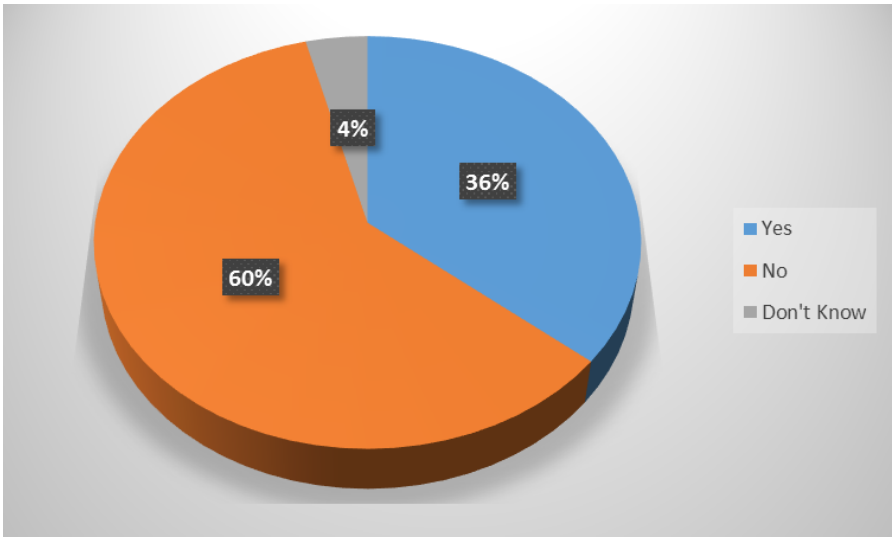
Do you think passwords are failing as an IT security method?



6. Learning to Share

More than one in three IT security professionals polled at RSA Conference 2016 admit that their IT staff share passwords. It's a common IT administration practice. Looking to cut corners and simplify matters, systems administrators often re-use the same password across multiple systems and among multiple IT administrators. While convenient for the IT staff, if a hacker or malicious insider gets hold of this common, shared password, he's just gained access to systems throughout the network.

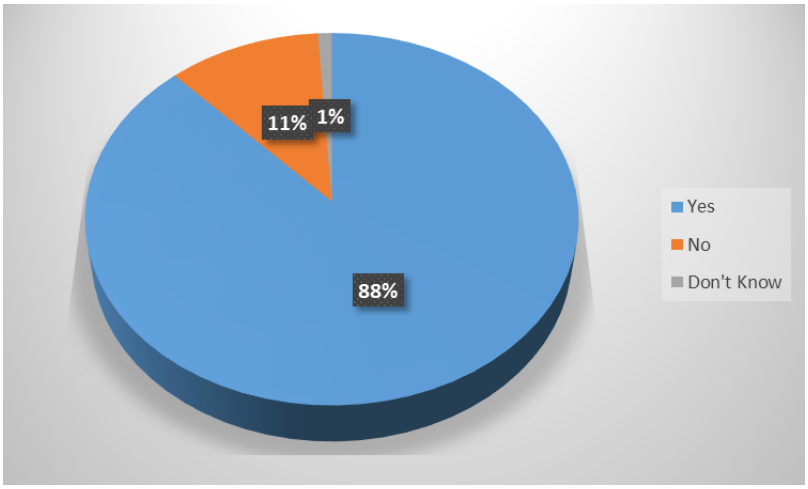
Are there cases within your organizations where IT staff share the same password?



7. The Default Fallback

Many hardware devices, applications and appliances – like firewalls and UTMs – come pre-configured with default passwords that are publicly known. If these default passwords aren't changed, they're an easy access point for a hacker. Despite the fact that this security vulnerability has been well known for years, more than 1 in 10 survey respondents still work in places that don't always change these passwords.

Does your organization always change default passwords on IT equipment?

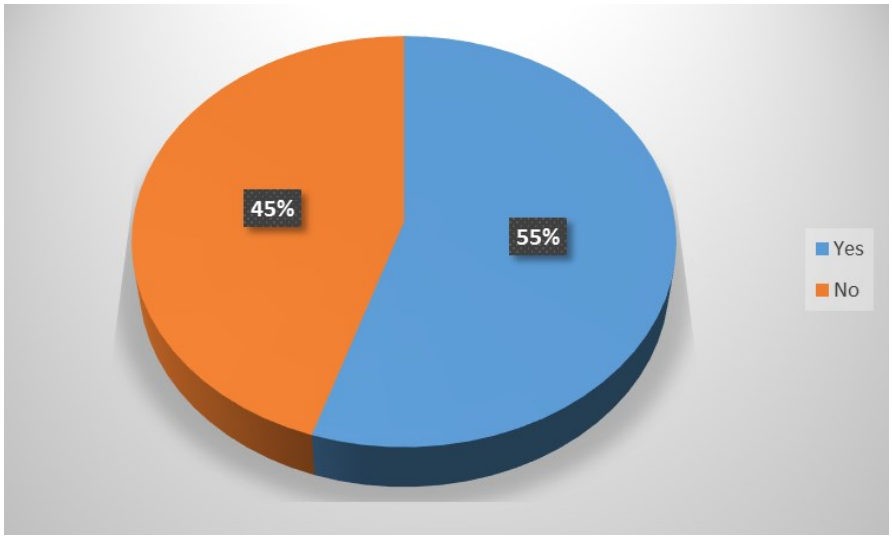


8. Preparing to Fail

Last year the cyber security market was estimated to reach $75 billion.1 How are these investments in security products paying off for organizations? Not well, apparently. Even when considering all of the IT security technology currently deployed in their networks, nearly half of respondents do not feel prepared to defend against a cyber attack.

Why the bleak assessment? It could be a response to current events. Major data breaches have filled the news over the past couple of years, and the frequency and severity of the attacks doesn't seem to be diminishing. Many of the breached companies invested heavily in conventional perimeter security tools - like firewalls and intrusion detection – to no avail. Zero days and other advanced threats can defeat perimeter security tools. Once inside the perimeter, all the intruders need to do is compromise just one privileged credential to move from system to system on the network, stealing sensitive data along the way.

Considering all the IT security technology your organization deploys do you think you are prepared to adequately defend against a cyber attack?

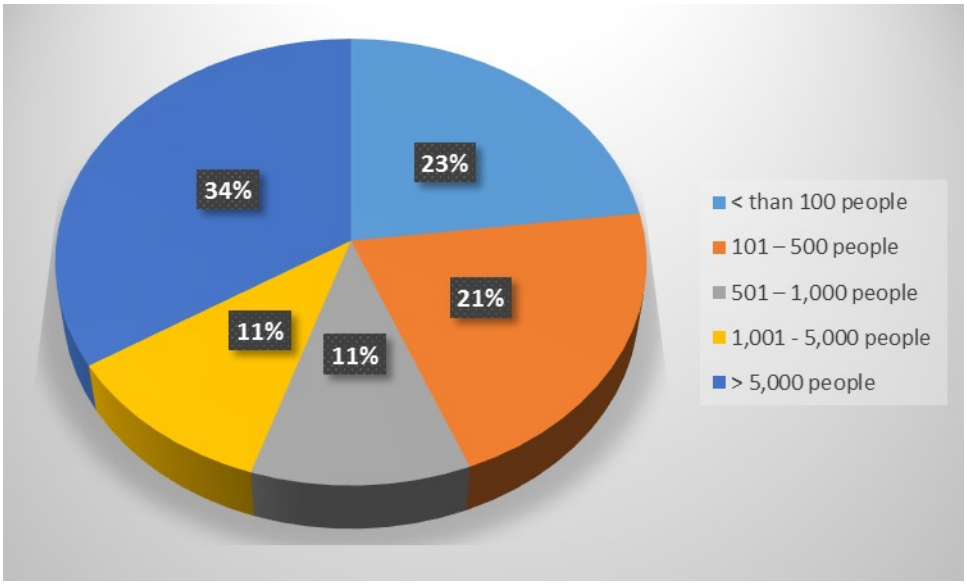


[1]*Forbes, Cybersecurity Market Reaches $75 Billion in 2015; Expected To Reach $170 Billion By 2020, Steve Morgan, Dec. 20, 2015*

Employee Size

45% of survey respondents work in organization with at least 1,000 employees.

What is the size of the organization you work for?



Survey Methodology

The survey was conducted among 190 attendees of RSA Conference 2016 in San Francisco. All responses were anonymous. Respondents were all registered attendees of the show and were polled one on one, on site during expo hours. Only fully completed surveys were measured for this report. Any incomplete responses were discarded by the tabulators.

About Lieberman Software Corporation

Lieberman Software proactively stops cyber attacks that bypass conventional enterprise defenses and penetrate the network perimeter. The company provides award-winning privileged identity management and security management products to more than 1,400 customers worldwide, including nearly half of the US Fortune 50. By automatically securing privileged identities – both on-premises and in the cloud – Lieberman Software controls access to systems with sensitive data, and defends against malicious insiders, zero day attacks and other advanced cyber threats. Lieberman Software is headquartered in Los Angeles, CA, with offices and channel partners located around the world. For more information, visit www.liebsoft.com.

LIEBERMANSOFTWARE™

www.liebsoft.com | P 800-829-6263 (USA/Canada) | sales@liebsoft.com
P (01) 310-550-8575 | F (01) 310-550-1152 (Worldwide)
1875 Century Park East, Suite 1200, Los Angeles, CA 90067

Published: March 2016