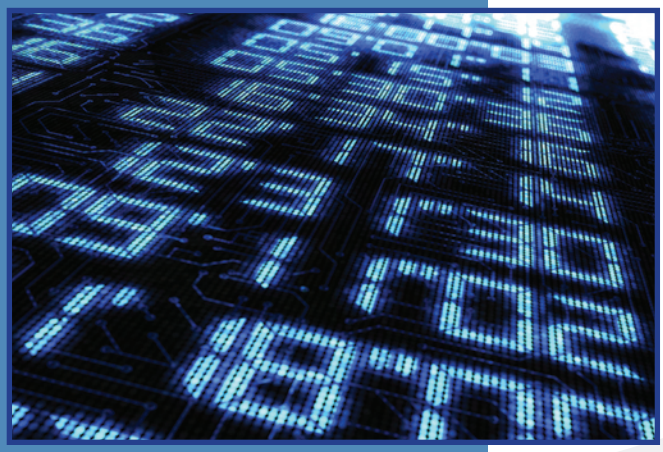

Best Practices for Information Security and IT Governance

A Management Perspective

LIEBERMANSOFTWARE

Strengthen Your Security Posture

The leading information security and IT Governance solutions go beyond simply satisfying auditor checkboxes, delivering an improved security posture and real business value. Lieberman Software takes information security to the next level with products that are uniquely designed to help you:

- Reduce your organization's risk profile
- Improve risk management operations through automation
- Lower the cost and uncertainty of IT regulatory audits
- Significantly reduce staff hours associated with implementing and managing Governance Risk and Compliance (GRC)
- Enable faster response to emergencies
- Minimize ongoing support and maintenance costs

Reduce Your Risk Profile

According to a Gartner study, worldwide IT security spending now outpaces every other area of IT investment[1]. Yet today's headlines suggest that many enterprises are losing ground when it comes to protecting their most sensitive data assets.

- A 2009 US Congressional report[2] states that "US government and private sector information, once unreachable or requiring years of expensive technological or human asset preparation to obtain, can now be accessed, inventoried, and stolen with comparative ease using computer network operations tools."
- A 2009 report[3] found that 70% of US financial institutions reported employee data theft in the previous 12 months.

Many of highest-profile data breaches reported in the press, including the cyber attack profiled in the US Congressional report, share an unsettling common characteristic. Attackers – whether insiders, intruders, or malicious programs – leverage unsecured "super-user" credentials to spread attacks throughout victim organizations.

Conventional IT security safeguards – including Identity and Access Management (IAM) frameworks, perimeter and endpoint security systems — do nothing to mitigate these types of attacks. The US Congressional report states that network attackers now "exploit this reactive defense model and they have the resources necessary to develop and exploit previously unknown vulnerabilities that are often are missed by signature-based IDS/IPS and endpoint protection software." For these reasons organizations are now fin ding it necessary to adopt new kinds of safeguards to secure their privileged identities.

Remove vulnerabilities caused by sharing privileged passwords and reduce your risk profile with **Enterprise Random Password Manager (ERPM)** from Lieberman Software. Manage, secure, delegate, audit and easily report on all privileged access throughout your enterprise – from the iron to the application.

[1] "Security Software and Services Spending Will Outpace Other IT Spending Areas in 2010," Gartner Group G00170482, August 20, 2009

[2] "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," The US-China Economic and Security Review Commission, October 9, 2009.

[3] "Bankers Gone Bad: Financial Crisis Making The Threat Worse," Dark Reading, October 5, 2009

Automate Risk Management Operations

Organizations rely on Lieberman Software to automate the processes required to:

- **Secure their infrastructure** and protect sensitive data against insider threats, malicious programs and unauthorized users
- **Demonstrate improved governance** by safeguarding privileged identities as required by major regulatory standards
- **Lower the cost of compliance** by creating all of the detailed, authoritative reports needed to document privileged access histories and demonstrate that all systems are protected.

Privileged identities are your so-called "super user" accounts that hold elevated permissions to access files, install and run programs, and change configuration settings. They exist on virtually every server and desktop operating system, business application, database, Web service, and network appliance in your organization.

Because privileged identities are present in so many places inside your IT infrastructure, it can be virtually impossible to secure them without automation. We have encountered numerous organizations that use waivers to prevent having to change certain accounts because they are so difficult and time consuming to change manually. In addition, IT administrators don't know everywhere privileged accounts may be in use so changing them might cause an operations failure – which means these account passwords never get changed.

With ERPM, you can automate the entire privileged credential change management process:

- Keep up with your dynamic environment through automated privileged account discovery
- Auto-discover everywhere privileged accounts are referenced
- Programmatically create and store complex, random passwords for privileged accounts in an encrypted repository
- Schedule privileged password change jobs to run regularly – at times and frequencies you designate
- Propagate changed passwords to all locations where those accounts are in use
- Feed all privileged access to auditing systems without human intervention
- Enable privileged access controls to be fed to strong authentication and remote connection systems
- Delegate, track, audit and easily report on all privileged account access

"Our biggest advantage is that our systems are now much more secure. Controlling our privileged identities helps protect us against threats like malicious software. Another benefit with ERPM is the time savings and increased productivity compared to scripting."

— **Shane Nicely** | VP Information Services
Heartland Financial USA

Lower IT Audit Costs and Uncertainty

Current industry mandates such as PCI DSS, Sarbanes-Oxley, HIPAA, FISMA and the like require you to document the presence of privileged identities in your infrastructure, maintain cryptographically strong privileged passwords, and to control and audit their use. These requirements cover virtually every type of organization and market.

Today, many organizations deploy ad-hoc methods including scripting, manual changes, and storing of privileged account credentials without the benefit of a secured, automated framework. This consumes enormous IT staff time and makes it impossible to tie individual users to the actions that they perform using these identities.

The result is that too many of your IT staff probably have anonymous, full-time access to all of the data on your network and the ability to alter configuration settings and run programs anywhere they choose. This makes documenting compliance difficult – and IT audit results uncertain.

ERPM provides comprehensive, real-time audit trails. Each time authorized IT staff request privileged access or recover privileged passwords for routine maintenance or emergency fire-call repairs, ERPM creates an authoritative audit trail showing the requestor, target system and account, date and time, location, and purpose of the request.

In addition, ERPM enables efficient compliance reporting. Whenever you are required to prove compliance, ERPM provides detailed reports at the push of a button that eliminate the manual effort it otherwise takes to document that all of your privileged accounts are secure.

Reduce IT Staff Workload

Secure privileged accounts regularly without manual intervention and eliminate the burden of manually producing compliance reports. When your security policies require frequent changes to privileged passwords, ERPM discovers, changes and audits these credentials immediately, eliminating hours of tedious, error-prone work.

Our customers experience a significant reduction in staff hours associated with privileged account password management after deploying ERPM. In addition, many of our customers are able to reduce contractor headcount. For those contractors who remain, ERPM controls and audits their access to the organizations critical IT assets.

Furthermore, as your integrated IT services expand, ERPM detects new application interdependencies and simultaneously deploys all changed credentials to avoid service disruptions and lockouts.

"Among the solutions that we evaluated, ERPM is the only one that can automatically discover every privileged account on our network, providing real advantages over the less effective, less reliable manual alternatives."

— **Jonathan Hughes** | User Systems Manager
University of Westminster

Enable Faster Response to Emergencies

No matter when authorized IT personnel need privileged access to perform routine tasks or emergency fire call repairs, ERPM grants the credentials securely and without delay, according to roles that you predefine, through a console that's accessible from any web-enabled device. With ERPM, you can:

- Respond to outages and emergency repairs within seconds by enabling your support staff to retrieve privileged account credentials in real-time, from a web browser
- Reduce privileged account access requests and retrievals to less than one minute
- Remove the need for manager approval since authorization workflows are pre-configured
- Audit all check-out activity and alert management to unusual events

Minimize Ongoing Support & Maintenance Costs

The privileged identity management solutions from Lieberman Software deploy quickly and deliver unmatched time-to-value while helping you to secure your network and lower IT costs. Compared to other offerings in this space, our deployments and upgrades can be implemented quickly.

The easy-to-use console and the ability for ERPM to automatically adapt to your environment keep your maintenance costs low. Furthermore, ERPM integrates out-of-the-box with numerous applications and devices including: ArcSight, ASP.NET, Microsoft SharePoint, Microsoft System Center, ObserveIT, Raytheon SureView, and Thales nShield hardware security modules. Custom integrations require additional — though minimal — efforts to implement.

How else do we lower ongoing support costs? With ERPM, you will immediately experience a drastic reduction in help desk support calls. You will also increase your success rates for desktop software deployments.

Finally, manage your environment with minimal system overhead and keep up with your dynamic environment through automated account discovery. We've said it before but we'll say it again: automation is paramount! Once you've configured and deployed ERPM, it will operate cleanly and require minimal ongoing administration.

Automate Your Information Security Operations Today

Why wait? Enable your IT staff to spend time on business-driven technology initiatives that will ultimately improve company operations instead of manually changing privileged account passwords and assembling compliance reports. Contact us today to better understand how our solution might benefit your organization.

Contact Lieberman Software at **(800) 829-6263 (Toll Free USA/Canada)** or **Worldwide (01) 310-550-8575** or **sales@liebsoft.com** for more information or to request a no-obligation software trial. **Visit us online at liebsoft.com**.

About Lieberman Software

Lieberman Software provides privileged identity management solutions to secure the world's largest cross-platform enterprises. By automating time-intensive administration tasks, Lieberman Software increases control over the IT infrastructure, reduces security vulnerabilities, improves productivity and ensures regulatory compliance.

Lieberman Software pioneered the privileged identity management market, having developed its first product to address this need in 1999. The company is headquartered in Los Angeles, CA and has an office in Austin, TX.

LIEBERMANSOFTWARE

www.liebsoft.com | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152
1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067