



Securing the Information Businesses Rely On

FOR IMMEDIATE RELEASE:

CONTACT:

Jan Tarzia
Nadel Phelan, Inc.
831-440-2404
jan@nadelphelan.com

Trish Schaefer Reilly
IPLOCKS, Inc.
408-383-7513
treilly@iplocks.com

SEVEN LAWS OF INFORMATION RISK MANAGEMENT

Guidelines Help Organizations Achieve Compliance and Mitigate Risk Associated with Security Breaches

SAN JOSE, Calif. – May 24, 2005 – IPLOCKS™, the leading provider of enterprise information risk management solutions, today announced the Seven Laws of Information Risk Management. The Laws are a common sense framework for how organizations can achieve compliance and mitigate risks, while better connecting people, process and technology. For more detail on the laws and tips on how to implement comprehensive Information Risk Management, please visit www.iplocks.com/7laws.php.

1. Your partners and employees will steal from you

As globalization and interconnectedness increases without proper vetting and security, employees, customers and trading partners can accidentally corrupt your data or cause regulatory compliance issues through misuse of the data. In the worst-case scenario, they can steal confidential data and sell it.

2. Bust up policy barriers

Security, auditing, regulatory affairs and privacy impact the entire organization and should not be kept in departmental silos. People, process and technology must be integrated.

3. It's all about privacy

Security is a building block for privacy, which is a major component of regulatory initiatives. For example, CA1386, HIPAA and GLBA in the United States and the Japan Information Privacy Law are primarily about privacy. The fundamental weakness to such laws is they cannot protect your brand, sensitive data, business continuity or financial position against a breach.

4. Don't stop working

Effective Information Risk Management should not radically alter work or its flow. Examples are rife of organizations implementing draconian policies that substantially reduce productivity and impair customer service, while providing questionable security benefits.

5. Don't spend foolishly

You must match the level of Information Risk Management investment directly to the level of risk. For each dollar invested, ascertain the quantitative and qualitative risk mitigated by the technology.

6. Be afraid – it will happen to you

Expect the unexpected by assigning responsibilities before a privacy breach occurs. Information theft only happening to the “other guy” is just a myth and the chance is greater than 50 percent that it has already happened at your organization. Ernst & Young recently reported that 70 percent of all security breaches that involve losses of more than \$100,000 are perpetrated internally.

7. No silver bullet

There is no single technology that will solve security problems or provide regulatory compliance. Information Risk Management is a process that requires continuous monitoring, auditing and adjustment of how sensitive information is used — not just an initial risk assessment.

“The productivity and cost savings associated with relying on technology to streamline internal operations, better arm sales forces and communicate more effectively with partners and customers are enormous — and so are the risks,” said Akio Sakamoto, President, CEO and Co-founder at IPLocks. “Perimeter-based security, encryption, traditional security approaches and database management systems cannot stop the most lethal thieves, which are users with legitimate authorization. Only a strong solution based on user behavior can provide organizations with effective and reliable first and last lines of defense.”

ChoicePoint, LexisNexis and DSW have recently grabbed the media's attention. Each could have been avoided through proactive Information Risk Management and the potential resulting financial loss, customer defection, costly reputation damage, legal liability and disruption to business operations would have been minimized or prevented. If implemented properly, Information Risk Management can keep your company from becoming a headline.

Information Risk Management is about integrating people, process and technology to protect businesses critical data and intellectual property. If information leaks occur, effective Information Risk Management practices help organizations detect the breaches, catch and successfully prosecuting offenders, deter similar breaches and provide mechanisms for re-establishing data integrity.

Visit www.iplocks.com/7laws.php for the comprehensive Seven Laws of Information Risk Management version.

About IPLocks

IPLocks, Inc. protects business continuity; safeguards company brand reputation and eases the pain of corporate governance by securing critical information assets from negligent and malicious acts. The IPLocks Information Risk Management Platform alerts management to information risks from security and business policy violations, attacks on data, compromised structural integrity and information theft, which other security solutions fail to detect. IPLocks secures business critical data for financial services, telecommunications, media services, healthcare, public utilities and other industries. Founded in 2002, San Jose, California-based IPLocks is a privately held global corporation with customers throughout North America, Asia Pacific, South America and Europe. For additional information, visit www.iplocks.com.

###

IPLocks is a registered trademark of IPLocks, Inc. All other registered or unregistered trademarks are the sole property of their respective owners.