



VENAFI, INC.

INFOSECURITY 2011 ENTERPRISE KEY AND CERTIFICATE MANAGEMENT AWARENESS SURVEY

VENAFI SURVEY FINDS THAT A SIGNIFICANT PORTION OF IT STAFF
COULD WREAK HAVOC TO THEIR ORGANIZATION'S NETWORKS

Eliminating un-quantified and unmanaged security, compliance and operational risk—
Millions of encryption keys and digital certificates at a time

Copyright © 2011 Venafi, Inc. All rights reserved. Venafi, the Venafi logo and Systems Management for Encryption are trademarks of Venafi, Inc. in the United States and other countries. All other company and product names may be trademarks of their respective companies. This datasheet is for informational purposes only. Venafi makes no warranties, express or implied, in this summary. Covered by United States Patent #7,418,597, #7,568,095, #7,650,496, #7,650,497 and other patents pending

Executive Summary

Venafi is providing this free report to the market to demonstrate the challenges organizations are facing when it comes to data protection, encryption key and digital certificate management. Based on a detailed survey of 500 Information Technology and Security professionals at InfoSecurity 2011, the report draws conclusions about the risks, which organizations face from weak encryption key management practices and the lack of automation of encryption keys. The survey shows that organizations are taking huge risks with mission-critical and sensitive business data. This risk is reminiscent of the situation Anglo Irish Bank found itself in when ex-employees held the organizations' encryption [keys ransom](#) after they left the organization.

When organizations rely on the Internet and its corporate networks to conduct global business and facilitate worldwide communications, they deploy multiple layers of IT security hardware and software technologies — all designed to protect networks from unauthorized intrusions, cyber attacks and regulatory compliance violations.

Encryption key and digital certificate technologies are vital to any effective IT security and compliance program. These indispensable tools allow people, systems and servers to authenticate with one another, secure data, and validate that only authorized users and systems are conducting incoming and outgoing communications and business transactions. Sensitive, regulated information would be completely exposed without digital certificates and encryption keys.

All organizations that rely on electronic communications and authentication — regardless of size or industry — utilize encryption keys and digital technologies in some form. Many of the world's Fortune-ranked organizations utilize thousands and even hundreds of thousands of encryption keys and digital certificates across its global networks. Without automated management processes, solutions and best practices, organizations will never gain complete control of its key and certificate inventories. This results in significant unmanaged and un-quantified security, compliance and operational risks within an organization, including unauthorized access, failed security audits and unplanned system downtime.

This report and its conclusions are based on the following data point:

- A survey of 500 IT security specialists attending InfoSecurity Europe 2011.

Conclusions

This report provides a number of relevant general conclusions:

- A significant number of IT staff could cause chaos for their organizations with their knowledge of and access to digital certificates and encryption keys due to lack of management controls and no separation of duties
- Most organizations do not know where all of the encryption keys are kept in order to open or access its data
- Many employees have found themselves in the situation where they cannot find the encryption keys to open or access files or documents
- Most companies could be held to ransom by their staff even after they have left the organization
- Organizations are aware that they must take steps to encrypt their vital data assets
- The majority of organizations use encryption technologies, including symmetric keys, SSH keys, asymmetric keys and digital certificates
- Most organizations have manual processes in place to inventory, monitor and manage their encryption keys and digital certificates
- Most organizations are in encryption chaos – encryption keys are deployed and strewn throughout the organization, in a siloed fashion, and IT staff do not know where they are
- A large majority of organizations would like to automate the management of encryption keys but simply do not know that there are technologies available to do so
- A significant number of organizations are deterred from investing in encryption technology because of the fear of losing its keys, and therefore the access to encrypted data

Venafi InfoSecurity 2011 market survey results:

1. 82 percent stated that the company they worked for used digital certificates and keys
2. 43 percent said that they had tried to open or access a document or file but failed because it was encrypted
3. 36 percent said that they could hold their organization to ransom if they wanted to by holding back access to encryption keys, 49 percent said they could not and 15 percent said it was not applicable to them
4. 31 percent said that if they left, they could take the keys with them and still access sensitive information remotely, 53 percent said they could not and 15 percent said it was not applicable
5. 43 percent said that if they left the company they could still cause havoc with their knowledge of digital certificates and keys
6. 76 percent said that they would use a tool to automate the management of encryption keys while 12 percent said they would not use it