



Echelon One
Executive Security and Risk Services

VENAFI, INC.
CONDUCTED IN CONJUNCTION WITH:
ECHELON ONE

2011 IT SECURITY BEST PRACTICES ASSESSMENT SECURITY AND COMPLIANCE BEST PRACTICES & RANKINGS

DEMONSTRATING WHERE TODAY'S ENTERPRISES AND GOVERNMENT
AGENCIES RANK WHEN IT COMES TO BEST PRACTICES ADHERENCE

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 joined forces with IT security research firm Echelon One to establish a set of 12 IT security and compliance best practices and to evaluate where Global 2000 enterprises, government agencies and other organizations were succeeding or failing when it came to implementing critical standards. Venafi sponsored this research to better understand the state of digital security and compliance in the new era of modern IT in hopes that it might provide its customers and the security community as a whole with specific direction on how to reduce risk. Venafi similarly used these findings to improve its own product offerings and professional support services.

Results of the research are best expressed in the words of Echelon One founder and CEO Bob West, *“The assessment findings were startling. We suspected we would find that many organizations were challenged, but we had no idea that failure rates would run this high.”*

The findings raised the question: *In today’s cyber environment, where attacks and compromises are frequent and effective, why are organizations failing to adhere to best practices and standards in such monumental proportions?*

This research demonstrated that when enterprises, government agencies and other organizations rely on a combination of human management and technology solutions to protect critical digital information assets, seemingly irreconcilable gaps between security and access emerge. To close these gaps, organizations implement multiple policies, checks and practices. Yet this simple solution proves to be quite complex as organizations struggle to determine exactly what the most effective policies, checks and practices should be.

Should organizations encrypt all data in the cloud? How often should an organization conduct security and compliance training? Should SSH keys be rotated annually, semiannually, or within some other interval? When trying to answer these and other critical questions, organizations often times do not know where to turn for information and guidance, nor do they know how to train their staff, rotate keys, or encrypt data once they get the answers.

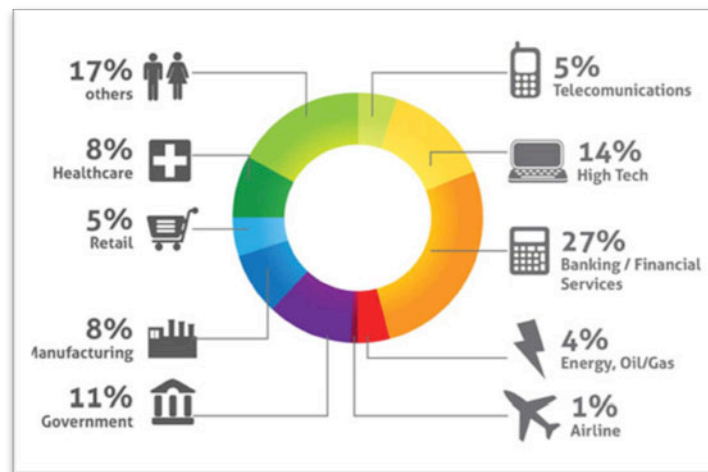
Through this research and related findings, organizations can receive specific guidance on what their top IT security and compliance best practices should be, how they stack up against the competition in terms of best practices adherence, and what steps they can take to close the security and compliance gaps that human error and a lack of automation continue to create.

Methodology

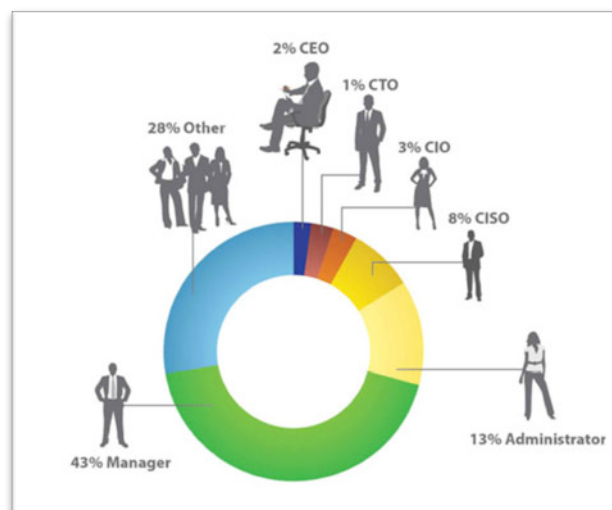
Questions and best practices baselines were established in conjunction with IT security research firm Echelon One, under the leadership of founder and CEO Bob West. To develop the evaluation and baselines, West drew on his constant interactions with Fortune 500 customers and 20-plus years of IT security experience in former positions such as CISO of Fifth Third Bank.

The research process included a survey of more than 420 participant organizations through an independent online survey conducted in July.

Respondent organization demographics:



Respondent demographics:



Top 5 Best Practices, Failure Rates and Recommendations

➤ Best Practice 1

✓ Perform quarterly security and compliance training. Failure rate — 77%

- Reason: There are many reasons why organizations are failing at this best practice. Among them are a lack of resources, knowledge and time.
- Recommendation: To make up for this shortfall, deploy technologies that compensate for lack of training resources by removing opportunities for human error through automation.

➤ Best Practice 2

✓ Encrypt all cloud data and cloud transactions. Failure rate — 64%

- Reason: Salesforce.com, Google Apps and other cloud applications do not encrypt by default. Most organizations fail to realize the vulnerabilities of data in the cloud.
- Recommendation: Deploy third-party technologies that encrypt cloud data—both in motion and at rest—to enhance security, compliance and privacy.

➤ Best Practice 3

✓ Use encryption throughout the organization. Failure rate — 10%

- Reason: Encryption is widely accepted as one of the most hardened security technologies. In fact, most organizations accept it as basic to their security strategy. Although the low failure rate seems encouraging, failure to implement management technologies can turn encryption into a liability by exposing keys and certificates that provide unrestricted access to seemingly secure data.
- Recommendation: To reduce the risk of encryption turning into a liability, deploy technologies that can manage encryption assets across the entire enterprise.

➤ Best Practice 4

✓ Have management processes in place to ensure business continuity in the event of a Certificate Authority (CA) compromise. Failure rate — 55%

- Reason: Most organizations do not realize that they are responsible for replacing compromised certificates deployed in their environments. Digital certificates rank among the most ubiquitous security technologies in use today.

Recent CA breaches demonstrate that certificate authorities have been and will continue to be compromised.

- Recommendation: Using a CA is only half the battle. To further reduce risk, have a plan for immediately replacing all certificates and encryption keys generated by a compromised CA.

➤ **Best Practice 5**

- ✓ **Rotate SSH keys every 12 months to mitigate the risk incurred by average two-year employee turnover rates of service. Failure rate — 82%**

- Reason: Enterprises that do not rotate keys fail to understand their significance and related security vulnerabilities. They are also unaware of automation technologies that can simplify the process. SSH keys provide root-level access to critical systems and data. A key-rotation period that far exceeds the average employee's lifecycle significantly increases the risk that a former employee or malicious admin can gain unfettered and unauthorized access.
- Recommendation: To make timely key rotation possible, deploy technologies that simplify and automate key rotation.

Best Practices 6 – 12 and rankings

➤ **Best Practice 6**

- ✓ Use 2048 bit encryption for symmetric keys and at least 256 bit encryption for asymmetric keys.
 - 17% achieve symmetric key best practices, using 2048
 - 27% achieve asymmetric key best practices, using 256
 - 56% do not use the recommended key lengths
 - 20% do not know the length of keys deployed

(*January 2011 research from NIST indicates 1024 bit keys have depreciated.

<http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>)

➤ **Best Practice 7**

- ✓ Maintain compliance with regulations and encrypt all transactional, employee, customer, and intellectual data.
 - 25% exceed best practices by encrypting all data types
 - 45% achieve best practices by encrypting based on regulations and by encrypting transactional, employee, customer and intellectual information

- 30% do not encrypt data types that should be encrypted
- 9% do not know what data types they encrypt

➤ **Best Practice 8**

- ✓ Separate duties for administrative access to encryption keys.
 - 69% achieve best practices, separating duties for administrative access to encryption keys
 - 31% do not separate these duties or do not know if their organizations have separation of duties for administrative access to encryption keys
 - 16% do not know if they have separation of duties

➤ **Best Practice 9**

- ✓ Manage all noted security processes to minimize enterprise exposure to unquantified risk; security processes requiring management include:
 - Change Management
 - Patch Management
 - Vulnerability Management
 - Encryption Key Management
 - IP Address Management
 - Server Traffic Management
 - Network Management
 - Configuration Management
- 55% achieve best practices, managing all processes
- 45% are not managing all processes

➤ **Best Practice 10**

- ✓ Perform an annual assessment of security and risk management programs
 - 68% achieve best practices, performing security and risk assessments at least once per year
 - 32% of organizations are performing security and risk assessments too infrequently or do not know how frequently or infrequently they are being performed
 - 16% do not know when the last security and risk program assessment was conducted within their organization

➤ **Best Practice 11**

- ✓ Conduct vulnerability assessments once per quarter
 - 69% achieve best practices, running vulnerability assessments with recommended frequency
 - 31% don't know how regularly vulnerability assessments are conducted in their organization

➤ **Best Practice 12**

- ✓ Address and assess risk associated with security, compliance, and operations to quantify a risk profile and respond accordingly
 - 74% are addressing and assessing security, compliance, and operational risk
 - 26% are not meeting risk management best practices

Unknown Risk:

The assessment further revealed that almost 100 percent of evaluated organizations had some degree of unknown security, compliance or operational risk.

- When asked if their organizations encrypted data stored in leading public clouds such as Google Apps, Salesforce.com and Dropbox, 40% said they did not know.
- When asked how often critical encryption assets such as SSH keys were rotated, 41% responded that they did not know.
- When asked if their organizations were using encryption keys and certificates for data security and system authentication, 10% said they were not.

Assess your organization:

To access the complete assessment and executive summary or to assess your organization, visit: www.venafi.com/2011assessment. To take the survey in-person or to discover how to achieve best practices for your organization, visit Venafi at Black Hat USA 2011, August 3 and 4 at Caesars Palace, Las Vegas, NV, Booth 701.

How Venafi can help:

Venafi is the market leader of enterprise key and certificate management (EKCM), and delivered the first enterprise application to automate the provisioning, discovery and monitoring of encryption assets across heterogeneous environments. Venafi solutions automate processes that mitigate human errors and simplify complex management problems. If your organization is in need of process automation that reduces unmanaged and unquantified risk, Venafi can help.

Contact Venafi:

- For immediate assistance, please contact us at sales@venafi.com or call 801.676.6900.
- Worldwide Headquarters
126 W Segoe Lily Drive #126
Sandy, UT 84070, USA
- Phone +1.801.676.6900
- Fax +1.801.676.6901

www.venafi.com