Ten Key Management Mistakes... and How to Avoid Them

A Futurex Whitepaper

Introduction

Data encryption and security is becoming increasingly important for enterprises of every size. It has moved from the realm of a "want to have" to a "need to have" based not only on emerging industry compliance mandates, but on the increasingly interconnected and sophisticated world around us. Every day, those who wish to breach your information systems are becoming more sophisticated and cunning in their methods. It's important not only for your business goals, but also for the soundness of your customers' sensitive information to make sure your key management system is the best that it can be.

The purpose of this whitepaper is to educate those who are new to the area of encryption key management or provide a fresh perspective or "food for thought" for those with more advanced knowledge of the topic.

Definitional guides can be found elsewhere. Instead, *Ten Key Management Mistakes... and How to Avoid Them* relies on everyday situational problems that IT professionals encounter in the course of ensuring the security of their systems, along with a framework of solutions and strategies for how to deal with them. Sometimes these are found in the data encryption industry, and sometimes from organizational management. It is important to remember that key management is not just about the technology, though these solutions and their features are extremely important. The people who manage the solutions and implement the policies are the ones who decide the success, both in the short and long term, of your cryptographic system and your organization as a whole. Hopefully this whitepaper will serve as a guide for those seeking to implement a key management solution complete with a cohesive strategy and solutions suite to protect your enterprise and its vital data.

Mistake #1: Disregarding Split Knowledge and Dual Control

When searching for a key management system, organizations go to great lengths to find the correct solution for their infrastructure, doing careful side-by-side analyses of products, meticulously considering integration into current systems, and evaluating the scalability of the solution for the future. In the midst of doing all of this research on the front end, the establishment of day-to-day procedures for key management tends to be less fully realized. When this is the case, organizations run the risk of endangering the basic soundness and security of their overall key management system.

An organization's key management policy, as it relates to key management personnel, should be governed by the principles of split knowledge and dual control. These are the basis of an effective key management framework.

Dual Control

Within the scope of key management, dual control is the utilization of two or more people, operating in concert, to protect sensitive functions or information. None of the people involved have authority over any of the others in respect to the control of information or job responsibilities. It is vital that one key administrator not report to another. The objective of dual control is to ensure that no one person has consolidated power over sensitive information or sensitive tasks. A practical example of this is the necessity of two or more users to input password information or other unique credentials to access information in a given system (ASC X9 TR-39, 2009).

Split Knowledge

When applied to key management, split knowledge is a condition under which two or more parties separately and confidentially have custody of key components of a single key. Individually, each component conveys no information of the resulting cryptographic key. A primary example of the utilization of split knowledge is the generating and/or loading of the Master File Key. Best practices state that each component, of which there are multiple parts, should be held and entered separately, with no other person having access to or knowledge of the other parts (ASC X9 TR-39, 2009).

(Continued on following page...)

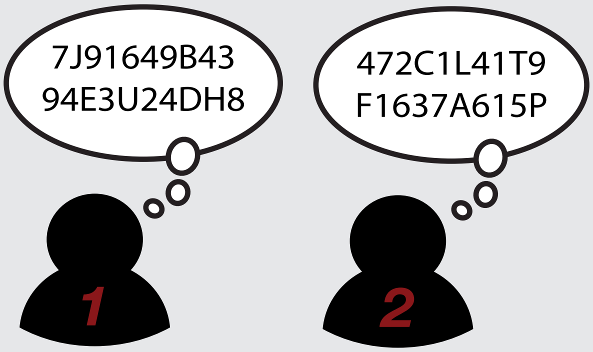
Key Management in Action

Step 1:

Create the key

Step 2:

Divide components between multiple key holders



Step 3:

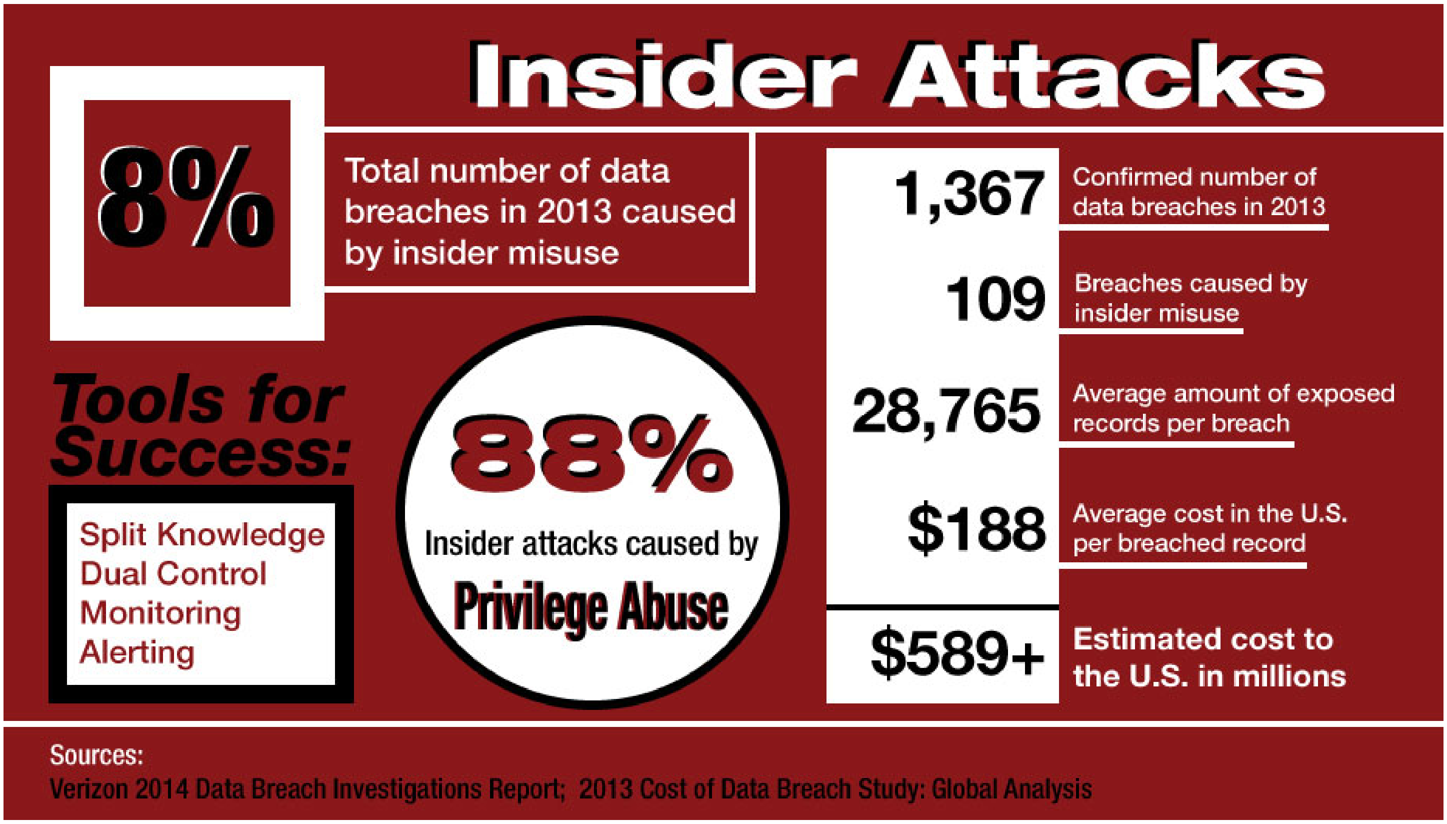
Separately enter components to recombine key during loading ceremony

(... continued from previous page)

The objective of these strategies is a decentralization of data, providing fewer or no instances of sensitive information recognizable to humans outside of a Secure Cryptographic Device (SCD). How can these practices be incorporated, at a high-level, into your organization's key management? Here are pertinent questions you can use to evaluate the soundness of your key management policy:

1. Do our key management systems enforce dual control during log in?
2. Do our key loading ceremonies require each key component to be entered individually?
3. Do any key holders know more than one key component?
4. Do any key administrator have undue influence over component holders?
5. Are there instances where split knowledge is compromised or not applied properly?

Leveraging split knowledge and dual control is essential to keeping your key management system secure. According to Verizon's Data Breach Investigations Report, almost 11,700 incidents last year were the result of insider and privilege misuse, and 22% of those instances took days to uncover. Monitoring your employees and placing reasonable restrictions on their key knowledge can save your organization millions.



Insider Attacks

8% Total number of data breaches in 2013 caused by insider misuse

1,367	Confirmed number of data breaches in 2013
109	Breaches caused by insider misuse
28,765	Average amount of exposed records per breach
$188	Average cost in the U.S. per breached record
$589+	Estimated cost to the U.S. in millions

Tools for Success:

Split Knowledge
Dual Control
Monitoring
Alerting

88% Insider attacks caused by Privilege Abuse

Sources:
Verizon 2014 Data Breach Investigations Report; 2013 Cost of Data Breach Study: Global Analysis

Mistake #2: Playing Fast and Loose with User Permissions

User permissions can greatly affect the success or failure of an organization's core cryptographic infrastructure, making instigating sound policies for the assignment of user permissions a vital component of key management.

One of the behaviors that introduces an element of risk to the soundness of a key management system is assigning responsibilities on a piecemeal basis. When employee permissions are assigned based on the tasks at hand rather than in the larger scope of a user permissions policy, managers significantly add risk into the security of their core cryptographic infrastructures. Permissions (used here to refer to access to resources) can be a complicated business for organizations of any size. Take for instance the chart of typical user permissions below. In a large enterprise, it's easy to see how role assignment can quickly become a jumble of checked toggle boxes.

Example of User Permissions

Permission	Description
Manage Keys	Add, edit, remove, import, and export keys
Manage Certificates	Add, remove, import, and export certificates
Manage Devices	Add, remove, and import devices and device groups
Function Blocking	Enable and disable access to specific API functions
Manage Users	Add, edit, or remove an individual user
Manage User Groups	Make changes to groups of users, including adding or deleting users or changing group permissions
Update System Configuration	Make updates to the system configurations
Create Notifications	Design and implement notifications for various events (e.g. technical difficulties, key expirations, certificate expiration)
View Logs	View, configure and maintain logs used in auditing
Backup and Restore Database	Use backup and restore functionality for system databases
Print Keys	Define templates and print key mailers

One of the most effective user permission strategies and a clear principle to have in mind when assigning user permissions is the principle of **least privilege**. According to the principle of least privilege, employees should only have access to the permissions and resources needed to reasonably complete their responsibilities. For example, in the table above, those who are administrators of the entire system would feasibly have all the user permissions enabled, but those who only need to input keys should not be able to create and delete user accounts.

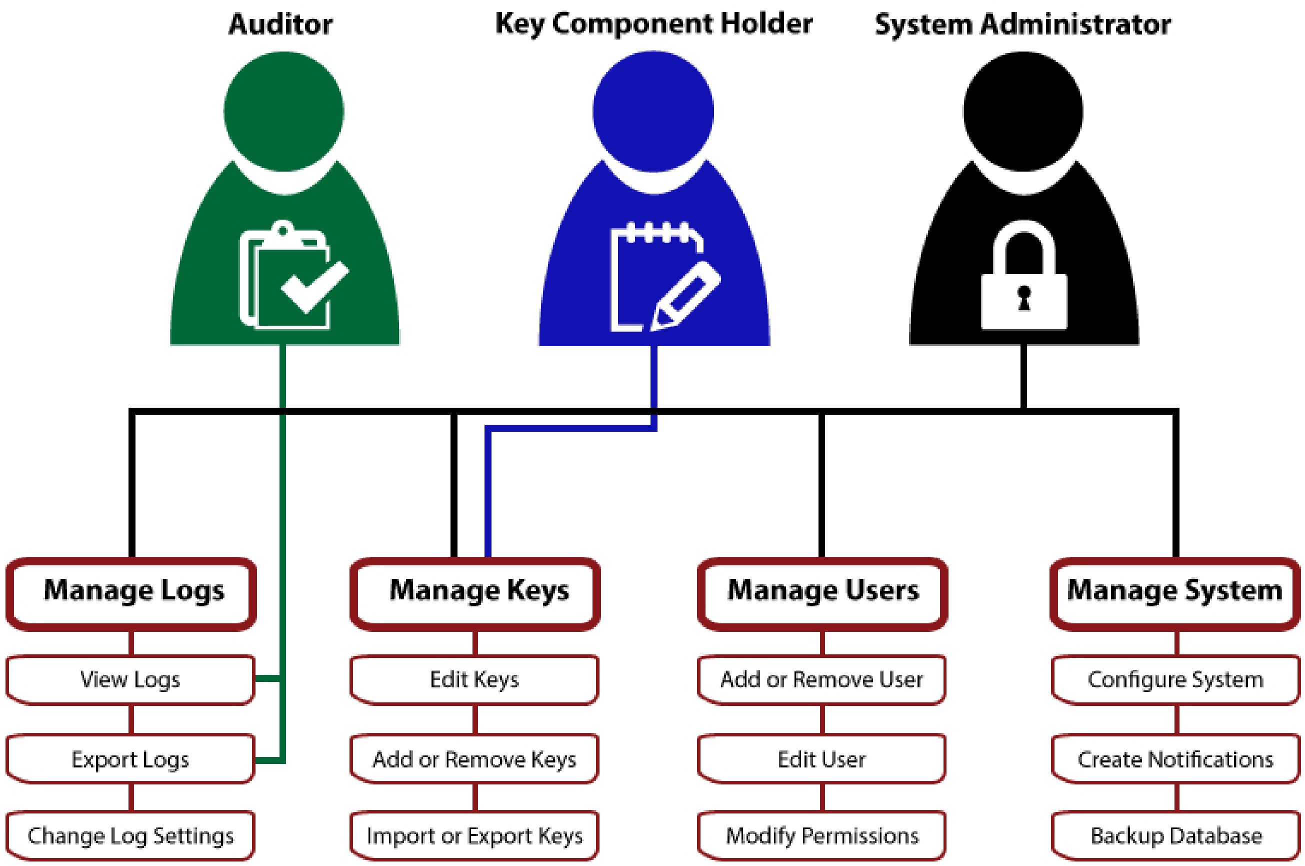
The concept of least privilege and user hierarchy has been around for the better part of 20 years and remains one of the most important concepts for secure key management. When assigning user permissions to those in your organization, it is useful to have these ideas in mind:

- As a part of a proper user permission hierarchy, permissions should only be assigned to roles based on the requirements of job functions and/or the entitlement of job qualifications.
- Users should have only as much access to systems as needed to complete their jobs.
- User permission constraints can and should be applied to enforce high-level security objectives to avoid being assigned two conflicting roles.

(Continued on following page...)

(... continued from previous page)

Another important principle to keep in mind is that of **separation of duties**. This means that no one person should be able to control all aspects of a key management task. Tasks should be divided among separate people. This concept is related to dual control, which is discussed in detail in the first key management mistake section. The below image illustrates proper separation of duties:



In the image, the key component holder, who is responsible for loading keys, has all of the key management user permissions. This person is not responsible for conducting auditing of the system and monitoring log files, so those permissions are not authorized. Instead, the ability to view and export logs is assigned to the auditor role. The system administrator, who is responsible for configuring and managing the entire system, has permissions for all roles. At the heart of this is the concept that users should only have access to the information they need to reasonably perform their jobs.

Because of the nature of high professional mobility today, it's important to conduct internal reviews at regular intervals to evaluate and re-evaluate whether the current user permissions of employees are in line with their job responsibilities. As roles are often reassigned within an organization, with new employees being integrated and other employees leaving, the initial user permissions scheme can look quite different from one year to the next. What is crucial for the success of least privilege is to avoid assigning user permissions based on individual jobs. Otherwise, the integrity of your planning can unravel quickly.

Mistake #3: Overestimating the Ease of Network Architecture Design

Industry experts use the familiar and apt comparison of network architecture to that of a house. Unless you're an expert, chances are that you won't attempt to lay your own foundation. Why would you try to do the same with encryption key management? Whether you're attempting to develop a key management network from scratch, or you're simply looking for ways to improve an inefficient system, network architecture deserves your respect and attention.

Keeping adversaries at bay in a world increasingly centered around advanced technology is a daunting task. Unfortunately, there are no shortcuts available when it comes to the security of your sensitive data.

Luckily, enterprises are not alone in this battle. Rest assured that the people at work in your competitor's network security center are tossing and turning at night mulling over the same or very similar security issues. There are a couple of actions you can take to make sure you have all the information you need to make an informed decision.

1. Start by tapping all resources

If you're scraping by with the bare minimum of funding, employees, and technology, the odds are that your network is not as strong as it should be. Compliance is more than just a checklist, and the road to secure architecture can be a winding one, but there are multiple avenues to implementing measures to ensure both short and long-term success. Leverage your resources and consult as many experts as possible to devise the best course of action for your organization and its unique needs.

2. Plan for the future

Key management is here to stay. Your organization's key management solution is not something that can be set aside and forgotten, even once you've passed your audits. Many organizations that suffer data breaches passed their compliance audits, but afterward let their security procedures slack or made changes to their infrastructure, leading to a breach. It's incredibly important to set a proper foundation for key management now and implement scalable solutions that will be able to grow and adapt as your enterprise, compliance measures, and industry best practices all continually evolve.

3. Have a backup plan

No matter how "bulletproof" technology is, there are still unexpected "oops" moments. For example, what if a tired technician spills coffee into a primary network switch? Your key management system may still be perfectly fine, but not online. What do you do then? Your organization likely cannot afford to have its key management system offline for an undetermined amount of time, so having a backup plan that can be immediately implemented to fix the situation is vital.

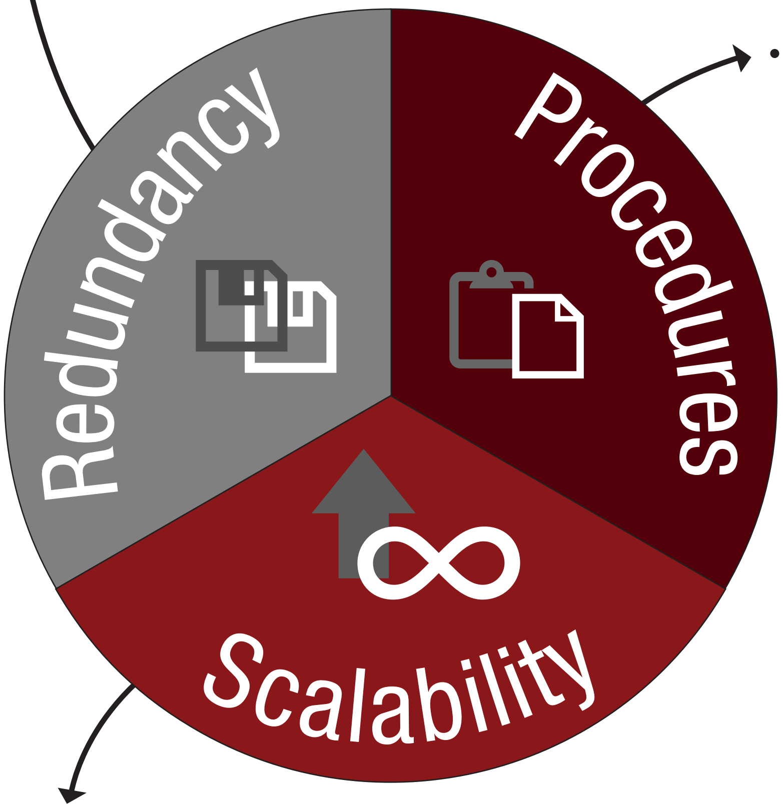
Certain situations are unavoidable. What matters is the sort of plan you have in place for such an event. At the very least, infrastructure should take into consideration redundancy and disaster recovery capabilities, backup and restore procedures and logistics, and scalability.

(Continued on following page...)

(... continued from previous page)

- **Redundancy and disaster recovery capabilities**:
  It's true that implementing redundancy can result in additional costs, but when the downtime of your key management system can be measured in millions of dollars, it's worth it. These mission critical systems require near-flawless uptime, which can be achieved by designing redundancy into the system.

  Standby redundancy is recommended and can incorporate some variations of cold and hot spare units. In a cold spare, a separate device or portion of your key management system is powered off until it is needed. With a hot spare, the duplicate unit is on and waiting to take over immediately should the primary unit go offline. Transfer of functions between units can be smoothed over greatly with the help of additional monitoring and load balancing units.



- **On and off-site backup and restore procedures and logistics:**
  Make sure to plan for backup and restore procedures and plan accordingly. Periodic dry runs of procedures for system outages are recommended. Make sure frequent backups of systems are made and kept both onsite and in a geographically separate offsite location. This is recommended in cases of environmental disasters.

  Say an earthquake hits your area: your system may be compromised, but if it is backed up offsite, your information will still be intact. It is crucial to test backup systems. There's nothing worse than thinking you're covered in an emergency and then discovering that the backup system does not work as planned.

- **Scalability for planned and unplanned throughput growth:**
  Sometimes too much of a good thing really is too much. When planning your network architecture, make sure this is not the case. Make sure your system is scalable enough to accommodate planned high-demand times and the unexpected ones as well.

4. Remember that you're not alone

It's a good idea to have a complete understanding of the compliance mandates in your industry, but you don't have to keep a copy of the standards documentation on your nightstand. Reach out to those with experience with solution implementation in your industry and leverage their knowledge.

Mistake #4: Letting Key Management Manage You

Key management is not meant to be easy; its primary function is to provide security for your organization and its sensitive information. That being said, with the ever-expanding desire and regulatory obligation for organizations to protect their sensitive data, products have developed to make implementation more convenient. There are several features now available in products that can provide significant savings in both time and money.

Remote Key Management and Configuration

Having to travel across the world for routine key management procedures is often seen as a necessary expenditure, both in terms of time and money. For organizations with geographically dispersed data centers, implementation of remote key management and configuration can dramatically decrease cost associated with key loading, rotation, and other management functions. Look for solutions with the following features:

- **Remote key injection via Public Key Infrastructure (PKI) secured IP network:**
  For organizations managing the injection of keys into a large number of remote devices (such as Point-of-Sale terminals, ATMs, employee consoles, or other manufactured electronic devices), remote key injection can completely eliminate the expensive process of manually loading keys. In addition, using a PKI-secured connection offers substantial protection over standard connections.

- **Automated, API-driven key management:**
  Even with full remote key capabilities, certain repetitive tasks still require manual operation unless robust automation is implemented. Developing a host application to interface with your key management server's Application Programming Interface (API) can introduce numerous advantages.

  For example, in an environment where keys must be rotated at designated intervals, the host application can automatically send an API call requesting that a new key be injected, decreasing overall cost and time associated with injecting new keys and virtually eliminating the potential for human error.

- **Audit records:**
  No one wants to scramble when audit time grows near. Some key management solutions have built in audit records that are just a mouse-click away. This enables quick and easy access to audit records from multiple devices.

- **Web Access:**
  Keys can be managed from anywhere in the world through a remote web interface. Using a secure web browser, a web interface with your key management solutions is the next best thing to being on-site. Users should be able to manage configuration settings and view recent transaction logs.

- **Centralized Management:**
  Technology is available to take some of the worry out of monitoring data security hardware spread across multiple locations. Look for solutions that offer monitoring, load balancing, and alerting. A public key infrastructure (PKI) would be necessary to facilitate the secure and trusted communication among multiple devices.

(Continued on following page...)

(... continued from previous page)

User Interface

Today, there are a number of choices to suit your organization's needs for user interfaces, including a Graphical User Interface (GUI), a network-level API for automated, programmatic management, or both. Each option has its benefits; one may be better suited to your organization than another.

Because of the user-friendly interface, a GUI reduces the barriers associated with non-technical personnel becoming key administrators. Regardless of the level of automation that you incorporate, Master File Keys must still be loaded by humans in a dual control environment.

Following on the concept of dual control, it's a good idea to not concentrate all control of key administration within a single department where some personnel may have authority over others. By spreading responsibility among employees in different departments, the integrity of dual control remains intact. The downside of this is that employees who are tapped for key administrator responsibilities may not have experience in day-to-day IT operations. For these employees in particular, a user-friendly GUI will decrease the learning curve and make the key management process more enjoyable for all involved.

A network-level API is extremely useful for automation and enables organizations to reach the high transaction throughput rates attainable by products currently on the market. Because of the involvement of people in the process of key management, often an API cannot be used alone and instead must be incorporated in concert with a GUI.

Scalable and Extensible Solutions

When choosing a solution for your enterprise, consider future upgrades and changes. Can new licenses or software-based feature upgrades be added down the line? Can this be done without taking it offline or out of service? Considering these questions now will save you a headache later. It's also an excellent bit of criteria to use to evaluate the cost of solutions down the line. Products that initially may be more expensive up front may turn out to be more cost-effective when upgrades and other features are considered down the line, or vice-versa.

Notification and Alerting Technologies to Look For:

Syslog: With compliance regulations requiring more comprehensive security measures, syslog allows administrators to consolidate and monitor multiple logs and to keep an eye on users and system activity through a single, centralized management server.

SMS (Short Message Service): Administrators can automatically be notified on their mobile phone via text message if technical issues arise with their key management system.

SMTP (Simple Mail Transport Protocol): Using SMTP, administrators can set up routine e-mail notifications when keys or certificates are about to expire, or if there are technical issues within the system.

SNMP (Simple Network Management Protocol): With SNMP, a dedicated monitoring server can be set up to watch over key management devices and respond or alert administrators of technical issues, monitor performance output, and issue notifications.

Mistake #5: Not Passing the "Lottery Test": Planning for Vacation, Succession, and Sick Days

Your employees are valuable. One of the things that keeps managers of any organization up at night is wondering what would happen if key employees were to leave suddenly. This quandary is known as the "lottery test." How would an organization cope if a crucial employee suddenly struck it rich in the lottery and quit their job that afternoon, never to be heard from again? Would it be paralyzed or is there a plan of succession?

The lottery test problem can be a tricky situation to navigate, as the principles of best practice place considerable emphasis on the decentralization of information and roles. While it is true that not all is lost with the departure of one employee, a vital piece of your key management puzzle may be missing. There are a few strategies that can function as a failsafe if one of your critical employees were to suddenly depart.

Conduct Periodic Dry Runs

Organizations can start by using unexpected sick days as "trial runs" to practice contingency plans. Vacations and even extended sick leave, while not ideal, are manageable. The vital information your employees carry is not completely inaccessible. The real test is the complete, sudden, and permanent loss of an employee. How would you proceed then?

Designate Backup Users in the System

Part of general management succession planning suggests that organizations have a pipeline of talent ready and waiting in the wings to assume more responsibility. One of the benefits in considering the talent development of current employees is that they have the ability to assume extra roles and responsibilities within your organization.

Can employees who have previously served in this role step up in case of absences of employees currently assigned the task? Are certain certifications necessary to do the job? Keep these questions in mind when designating backup administrators.

Do Preemptive Training

Don't wait until you've lost an employee to begin training the replacement. By allowing the intended backup administrator to work with the current primary and familiarize themselves with the routine as well as decision making processes, interest is stimulated while increasing skills.

Lightening the Load: Utilize M-of-N Key Fragmentation

Within the scope of key management, situations like the lottery-winning employee are when M-of-N key fragmentation is especially helpful. Typically, if an organization has a number of key officers, all of them must be present for a key loading ceremony. This usually means that they must take time out of their schedule and often travel long distances.

With the implementation of M-of-N key fragmentation, organizations can select a number of required key officers for a key ceremony that is less than the total number of key officers. If a company has eight key officers, it can designate any number above one but less than the eight to be present for key loading ceremonies. With this feature in place, the loss of an employee is a minor inconvenience to your key management procedures rather than a major disaster.

Mistake #6: Falling Victim to "Check-Box Compliance"

This is an easy mistake to make. After all, compliance mandates such as TR-39 and PCI DSS are often designed as checklists. It's important to recognize that compliance mandates are incredibly nuanced, and measures can be implemented in numerous different ways based on your organization's means in order to meet the same compliance ends.

There's an industry adage that states "compliance is a journey and not a destination." With how quickly technology is evolving, organizations can never truly rest easy knowing their system is fully compliant now and in the future. Instead, organizations must be constantly vigilant when it comes to ensuring complete compliance. The thought may be scary, but regulatory mandates have a variety of avenues that can be taken to reach compliance. Tapping all of your knowledge resources is essential to creating an effective key management solution.

Industry experts should be consulted from the beginning of the key management solution procurement stage all the way through the integration and operations processes. Ideally this should include vendors or industry experts who are certified under the same criteria as the auditors themselves.

Passing an audit is merely a snapshot in time. Sure, you were compliant then, which hopefully means that your organization's information was safe and secure, but what about the rest of the time? Do you have the infrastructure in place now to ensure you will be compliant in the future?

Avoid the habit of viewing compliance as a process of checking off certain boxes and take a look at the big picture. Treat compliance as a checklist, and you run the risk of assembling a mish-mash of products. A cohesive, well-thought-out solution is far more effective than the sum of its parts. With the correct guidance from industry experts, you have the chance to implement a security solution that fulfills compliance regulations but also integrates into other functions of the enterprise.

With proper planning and strategic foresight, regulatory compliance does not have to be something that your organization must comply with or else face the consequences. Instead, treat compliance as the minimum amount of security measures necessary. The requirements are there to ensure additional security for your organization as well as add value and a sense of security for your customers.

Industry Knowledge: CTGA Certification

CTGA (Certified TR-39 Auditor) is a certification given to auditors and industry experts who have undergone extensive training and testing in the area of compliance auditing.

CTGA-certified professionals possess the skills to analyze any cryptographic environment and verify whether its current security measures are sufficient to pass an audit, and more importantly, assess whether the security measures and policies in place now will be sufficient to stop a data breach.

By hiring a CTGA-certified expert to review your cryptographic infrastructure on a habitual basis, typically before each audit but ideally every time a major change is made to the infrastructure, you'll not only be more prepared to pass your compliance audit, but also ensure your data security measures are at their peak performance.

Mistake #7: Being Satisfied with Meeting the Bare Minimum of Security Requirements

The data security world is constantly changing to keep up with new and ever-evolving attack vectors. Regulatory compliance measures aim to keep pace with this change but can often be a step behind. Just as costly, if not more, is a breach of security that, according to some estimates, can cost an organization on average $5.4 million*, not to mention the intangible costs associated with the damage to their reputation. Because of this, it's good to exceed the minimum level of security requirements in your field. There are several options for additional security to get you started in increasing your security.

Leveraging Dual-Factor Authentication

Also called two-factor authentication, dual-factor authentication is a strategy for authenticating identity, in which a user is required to present two or more identifying factors for access to a system. Most commonly, this includes a memory or knowledge factor (a user must know something, such as a password), possession of a certain object (such as a smart card), or an inherent genetic factor (something the user is, such as biometric factors like iris or retina scans or fingerprints).

Dual-factor authentication has become a part of our everyday lives and will only become more prevalent and complex with the evolution of security threats. This prevalence extends to using a debit card and PIN number to access account information and funds at an ATM. It would only be logical to utilize this best practice in the security of your sensitive data. The more sensitive the data, the more factors should be required to access it. The most common form dual-factor authentication tends to take is the utilization of a combination of username/password information and a smart card.

Implementing and Enforcing a Strong Password Policy

A security system is only as strong as its weakest link. One of the weakest points of any password-protected system is weak passwords that can be quickly and easily guessed. Every year studies are published revealing the most common passwords, and without fail, every year there are passwords like "password" and "123456" near the top of the list. Investing heavily in a key management system, only to secure it with weak passwords, is incredibly risky and borders on negligence. Keep these ideas in mind when implementing a strong password policy:

- Never use a password that can be found in a dictionary. Password hacking attempts often start with dictionary attacks when trying to access accounts. Changing "password" to "passw0rd" does not make you safe either. Attackers are likely to use password dictionaries, which contain collections of words with common character combinations.
- The longer the password, the better. Best practices suggest that all passwords should be at least six characters and should include case sensitive letters, numbers, and symbols.
- A password should be easy to remember. Writing down a password and sticking it on your monitor negates all your efforts for security. A "pass phrase" can make remembering complex passwords easier. For example, the sentence "I like to play soccer" could become "iL2plAs0cEr."

(Continued on following page...)

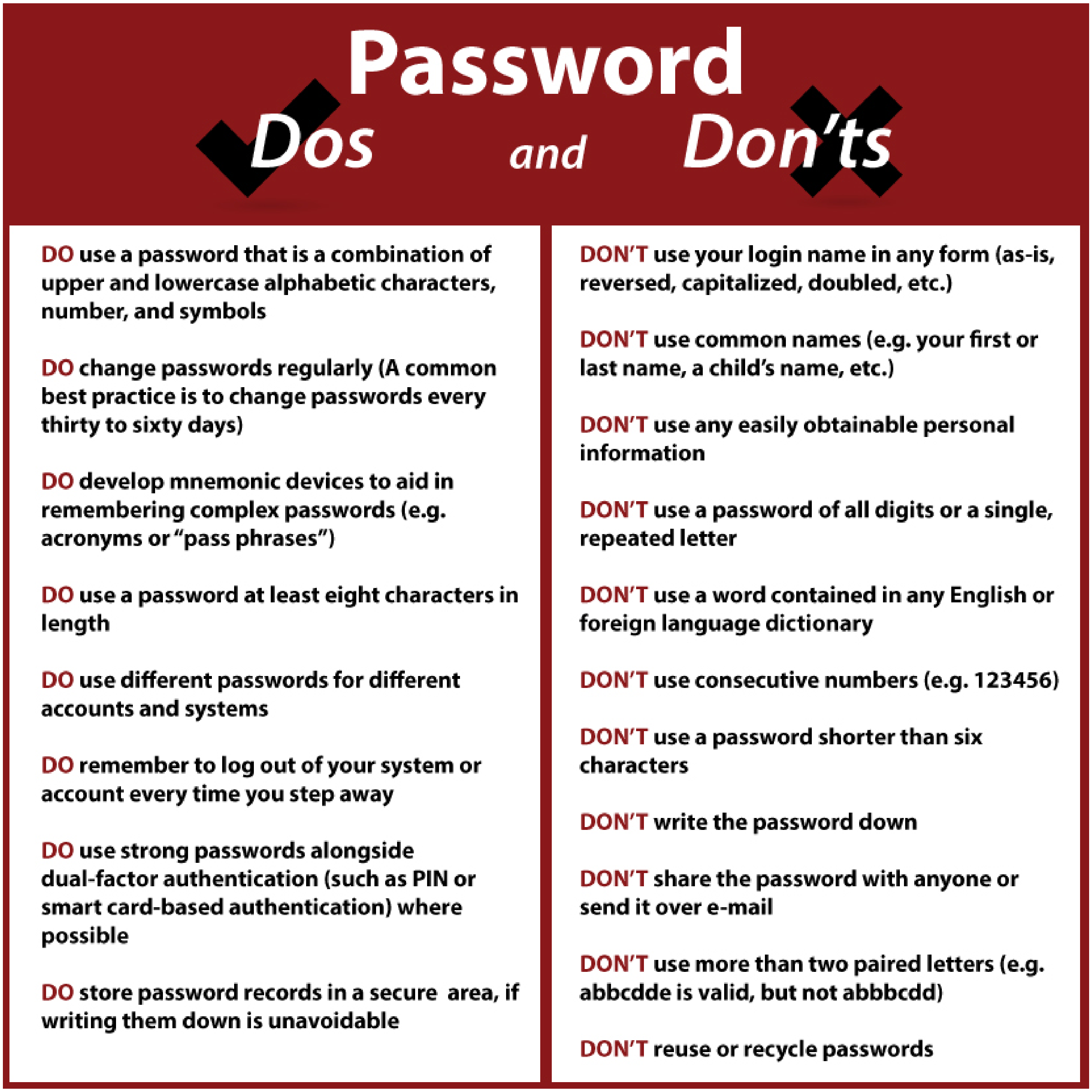
*2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute

(... continued from previous page)

Digitally Signing Entities with a TR-39-validated Certificate Authority

Formerly known as TG-3, TR-39 is a set of compliance guidelines published by the ANSI Accredited Standards Committee X9. These guidelines address the security of electronic transactions containing sensitive financial data.

By digitally signing all key management servers, host applications, and client endpoints using a TR-39-validated certificate authority, organizations have essentially authenticated the identity of all of these entities, creating a trusted and mutually authenticated environment. This is essential in a Public Key Infrastructure (PKI) environment to ensure that the identity of each portion of the key management system is authentic, protecting systems from substitution attacks.



Password Dos and Don'ts

DO use a password that is a combination of upper and lowercase alphabetic characters, number, and symbols

DO change passwords regularly (A common best practice is to change passwords every thirty to sixty days)

DO develop mnemonic devices to aid in remembering complex passwords (e.g. acronyms or "pass phrases")

DO use a password at least eight characters in length

DO use different passwords for different accounts and systems

DO remember to log out of your system or account every time you step away

DO use strong passwords alongside dual-factor authentication (such as PIN or smart card-based authentication) where possible

DO store password records in a secure area, if writing them down is unavoidable

DON'T use your login name in any form (as-is, reversed, capitalized, doubled, etc.)

DON'T use common names (e.g. your first or last name, a child's name, etc.)

DON'T use any easily obtainable personal information

DON'T use a password of all digits or a single, repeated letter

DON'T use a word contained in any English or foreign language dictionary

DON'T use consecutive numbers (e.g. 123456)

DON'T use a password shorter than six characters

DON'T write the password down

DON'T share the password with anyone or send it over e-mail

DON'T use more than two paired letters (e.g. abbcdde is valid, but not abbbcdd)

DON'T reuse or recycle passwords

Mistake #8: Not Educating the Stakeholders

Key management is not solely limited to the IT departments of organizations. Many of the most common key management mistakes can be mitigated by properly educating the organizational stakeholders.

Aside from the obvious technical and analytical skills necessary for a systems administrator, good communication skills are vital to success in this role. If the benefit of a robust, hardware-based key management infrastructure is not adequately conveyed to upper management, the implementation, operation, maintenance, and upgrade process will continually be more difficult than otherwise necessary.

Working in every system administrator's favor is the duty of upper management is to understand the lay of the land and make strategic decisions based on information available. To help reinforce the concepts that are vital to your organization, it is recommended to convene seminars, "Lunch-and-Learn" sessions, or a series of meetings to fully present all governing factors in your decision making.

Stakeholders should be informed on all aspects that would impact their attitudes, decisions, and job responsibilities. Some of this information is bound to recap aspects of key management that are already known; however, your task is to incorporate it in a way that clearly demonstrates the logic for your desire to implement a certain solution. By making a vested effort in stakeholder education, you can dramatically change the perception of regulatory compliance and security within the organization. This will result in an easier day-to-day job for system administrators, but more importantly, it will also lead to a greater organizational respect and valuation of security measures.

This includes, but is not limited to:

- **Compliance mandates and regulations as they apply to your organization**

  Your stakeholders are likely already aware of these regulations, but they will not be as familiar with the full technical ramifications of these mandates. Industry experts, vendors, or consultants with similar certifications to the industry auditors often have the ability to convey technical information in layman's terms, making it more likely that those without a technical background are able to fully grasp the situation.

- **Unique system environments**

  While industry best practices exist, each organization has its own unique features and culture depending on its strategy and business goals. It is best to utilize industry best practices but tailor them to your unique business and system requirements.

- **Future-oriented trends**

  It's impossible to know what the future has in store, but by consulting industry experts, you can be reasonably prepared for regulatory changes. It's also best to establish at the outset and build upon technology systems that are scalable and extensible. The investment you make now in technology can and should be able to evolve with the changes in regulatory mandates.

Mistake #9: Not Educating Front-Line Employees

It's true that an effective management policy starts from the top down by forming a cohesive plan. Once a policy has been decided upon, it's time to implement it where the rubber meets the road: with the front line employees.

A study by the security management company Rapid7 in conjunction with the Chronology of Data Breaches maintained by the Privacy Rights Clearinghouse* showed that most data breaches were not a result of outside attackers, as is most often assumed, but instead were due to negligence on the part of employees. The report showed that the 268 incidents profiled affected 94 million people, and most of these incidents were a result of negligence and clerical errors. This underscores the importance of properly educating employees on the security of sensitive data. Success of these key management policies and their widespread adoption and effectiveness hinge on the support of front-line employees.

If data security is not valued and highlighted by upper management, why would front-line employees treat data security measures any differently? The significance of these somewhat cumbersome tasks must be communicated to the employees often and with importance. These policy changes can be done through short seminars, lunch meetings, or educational sessions. By taking the time to instill the importance of tasks related to dual control, split knowledge, and other tasks that may seem to be inconvenient to users, mistakes often caused by confusion, apathy, or lack of education can be virtually eliminated.

It must be made clear to employees that the policies that may be more difficult than what they are accustomed to are not there to make their jobs more complex or difficult but to serve an important role to the employees, organization, and most importantly, the customers.

Keys to engaging employees to adopt these new procedures include:

- **Make it relevant**
  Employees should understand the background behind the procedures and what they are working toward. Often, the big picture can be lost in the midst of day-to-day tasks. They are more likely to take seriously the security measures if they understand the battle they are waging to keep the organization and its information safe and secure.

- **Be consistent**
  When implementing any policy, consistency is important, especially at the outset. Make sure information about the policy is prevalent and that there are numerous backstop checks throughout the process to ensure the new policies and procedures are thoroughly and correctly implemented.

- **Make it engaging**
  Let's face it: procedures aren't the most riveting facets of any occupation. Employees are more likely to absorb and enact policies when they understand the relevance and are engaged with the importance of their tasks. It's helpful to make the information session more engaging, but don't steer too far in the other direction either. You want the employees to remember the information and not the Jeopardy-style game you played, for example.

*http://www.rapid7.com/docs/data-breach-report.pdf

Mistake #10: Managing Encryption Keys in Software

Software key management platforms can be an alluring option, but it's extremely important to the integrity of your secure data to resist their boasted convenience. Software-based encryption programs are inherently flawed due to their vulnerability to malware, key logging, and other attacks that attempt to determine encryption keys. In the case of data security, the age-old view still proves true: a physically secure repository is still the safest place to store and process sensitive data.

Hardware-based key management solutions are a far more secure option for enterprises looking to sleep comfortably at night. Choosing a hardware-based key management solution validated to FIPS 140-2 Level 3 or higher provides for the best protection of the Major Keys used to encrypt all other keys within the system.

All FIPS 140-2 Level 3 or higher devices should include these important features:

- **Tamper-responsive circuitry that erases sensitive data upon detection of any intrusion attempt**
  Self-destruct sequences are not only for spy movies anymore; In this case, they're based in fact. To attain a FIPS 140-2 Level 3 or higher validation, the cryptographic module must be encased in sensor wires. If these sensors detect tampering attempts, the circuitry will zeroize all data contained with the module.
- **Physical security barriers that prevent access to internal components**
  Your key management technology should function as an impenetrable fortress. After all, this is one of the primary advantages over a software key management solution. The only place where the Master File Key is stored in plain text should be within the boundary of a Secure Cryptographic Device. Besides being surrounded by a protective, tamper-responsive outer casing, the hardware security module should also be secured by pick-resistant locks to prevent unauthorized access.
- **Digital signatures of cryptographic modules that prevent substitution attacks**
  Digitally signed cryptographic modules have undergone a process, ideally in a TR-39-validated environment, to authenticate the device's unique identity. This is necessary to ensure the identity of a device in a PKI environment and prevents substitution attacks, whereby an attacker attempts to insert another device into a trusted environment.

Public Key Infrastructure: Extra Layers of Security

A public key infrastructure is a method of asymmetric key encryption used to secure sensitive information, utilizing a pair of keys that are mathematically related. One key, the public key, is used by the sender to encrypt the message, and the other, the private key, is used to decrypt the information.

A problem that arises here is that any entity with the private key can decrypt the information. How can the other parties in this equation know that the other entities can be trusted? The other crucial part of this equation is the certificate authority, which issues digital certificates that validate the identity of the other entities, creating a circle of trust.

Sources and Recommended Further Reading

Bertino, Elisa, Byun, Ji-Won, Li Ninghui. A Critique of the ANSI Standard on Role Based Access Control. Purdue University, December 2007.

American National Standard for Information Technology – Role Based Access Control. ANSI INCITS 359-2004, February 2004.

Federal Information Processing Standards Publication 140-2. Security Requirements for Cryptographic Modules. NIST, December 2002

X9 TR-39-2009. TG-3 Retail Financial Services Compliance Guideline. ASC X9, July 2009.

2014 Data Breach Investigations Report. Verizon, 2014.

About Futurex

For over 30 years, Futurex has provided secure, robust, and cost-effective data encryption solutions for organizations worldwide. More than 15,000 customers have trusted Futurex's innovative technology to provide market-leading solutions for the secure encryption, storage, certification, and transmission of sensitive data. Futurex maintains an unyielding commitment to offering advanced, standards-compliant data encryption solutions, including:

- Hardware security modules for secure, reliable data encryption, information management, and key generation
- Remote key management and injection platforms
- Certificate authority issuance and management
- Secure, hand-held devices for configuration, management, and compliant key loading
- High availability solutions for load balancing, monitoring, and disaster recovery
- Secure storage and access of sensitive data

Throughout every facet of our organization, we maintain a focus on providing exceptional customer service, best-in-class technology, and cost-effective solutions for our customers. Our dedication to meeting the growing business needs of our global customers and partners is exhibited by the continuous expansion of our innovative products and services. Futurex has established technology partnerships with Fortune 500 organizations across wide-ranging industries, allowing us to provide value through integration with numerous data transaction networks. Through our results-oriented engineering culture, we have provided organizations worldwide with custom solutions supporting aggressive times to market.

Our products satisfy the most rigorous security requirements, and as we move forward, Futurex will continue to be a global leader in the data security and electronic transaction industries by maintaining high performance standards, providing quality service, and expanding our best-in-class product suite.

Questions? Contact us at info@futurex.com

GLOBAL HEADQUARTERS 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF 800.251.5112 P +1 830.980.9782 F +1 830.438.8782 info@futurex.com
WWW.FUTUREX.COM