In 2018 the evolution of computing and delivery platforms continues unabated at a rapid pace and this continues to present substantial challenges as organizations of all sizes to deploy data protection strategies. Lead by the General Data Protection Regulation (GDPR) in Europe, business leaders and security professionals now know that Data Centric Data Protection, or encryption, is crucial to their security and governance strategies. Deploying encryption naturally means properly protecting encryption keys. This is the biggest challenge organizations will face with their encryption strategy. The large investment required to develop defensible key management implementations, the importance of key management to critical data infrastructure, the rush to cloud and hybrid implementations, and evolving key management standards are ongoing concerns for every organization. Our predictions for 2017 have largely been confirmed and 2018 promises to continue in the direction we indicated last year. It’s dangerous, be safe out there!

Patrick Townsend, Founder & CEO, Townsend Security
CONTENTS

Encryption is Mainstream 4
Key Management is the Hardest Part of Encryption 5
Cloud Migration & Key Management Challenges 7
Virtualization Continues to Dominate IT Strategy & Infrastructure 8
Key Management Vendor Stability Still a Concern 9
Vendor Customer Support is an Ongoing Concern 10
Key Management as a Service (KMaaS) 11
KMIP is Finally Here 12
Key Management Systems Integration & Management 13
There is No Single Source for Best of Breed Security 14
Cyber Insurance is Evolving 15
Organizations will Continue to Fail Compliance Audits 16
Software-as-a-Service Application Vendors 17
WITH THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR) COMING INTO FULL FORCE IN MAY OF THIS YEAR, encryption of sensitive data, is now a high priority in most organizations. Historically investments in security have focused on deploying endpoint protection such as anti-virus and data leak protection, active monitoring and alerting of system logs, and other security features. Encryption is now a core security requirement, and many organizations are rushing to remediate a lack of attention to this area.

The large data breaches over the last three years and the resulting impacts on the executive teams, along with resulting brand damage, has changed everything. Customers, employees and all other stakeholders expect the highest levels of executive management to be pro-actively involved in the protection of sensitive data. When CEOs lose their jobs over a data breach, the industry is poised for change. Encryption and data protection are now considered cornerstones of a company’s governance, risk management, and compliance regime. Failures in data protection are now perceived as failures at the highest levels of management. Additionally, the State of California’s recent guidance that a minimum reasonable level of security requires the full implementation of the CIS Critical Security Controls, will force organizations to fully adopt encryption protections. Likewise, the New York Department of Financial Services prescriptive requirement for encryption of sensitive financial information is poised to take effect. This is leading to a rapid re-focus of the security strategy on data protection with strong encryption and key management.

TAKE AWAYS:

Review your defense-in-depth security strategy and move quickly to protect sensitive data with strong encryption and key management.

Be sure your IT department has a clear inventory of sensitive data across all of you internal systems, cloud solutions, and service providers. Know what is protected and what is at risk.

Prioritize your encryption projects to address the most sensitive and exposed data.

Every implementation of encryption needs good encryption key management. Start a remediation plan for any current encryption implementation that fails to properly protect encryption keys.

Communicate your security strategy to your customers, employees and stakeholders. Let them know that data protection is important.
WHILE ORGANIZATIONS ARE NOW COMMITTED to implementing encryption, they are still struggling with getting encryption key management right. With all major operating systems, cloud platforms, and virtualization products now supporting encryption, it is relatively easy to make the decision to activate encryption to protect sensitive data. But an encryption strategy is only as good as the method used to protect encryption keys. Most audit failures for customers already using encryption involve the improper storage and protection of encryption keys. Ignorance and fear are the driving reasons for this core security failure. Many IT professionals are still not versed in best practices for encryption key management, and IT managers fear that the loss of encryption keys or the failure of access to a key manager will render their data unusable. This leads to insecure storage of encryption keys in application code, unprotected files on the data server, and poor protection of locally stored keys.

Most encryption key management solutions have evolved over the last decade to provide unparalleled reliability and redundancy. This has largely removed the risk of key loss in critical business databases and applications. But the concern persists and inhibits the adoption of defensible key management strategies.

**TAKE AWAYS:**

Protect encryption keys with single-purpose key management security solutions.

Never store encryption keys on the same server that houses sensitive data.

Avoid cloud service provider key management services where key management and key custody are not fully under your control.

Only deploy encryption key management solutions that are based on FIPS 140-2 compliant technology.

Only deploy encryption key management solutions that implement the KMIP industry standard for interoperability.

Download eBook

Encryption Key Management Simplified
Automatic high availability failover to one or more secondary hot key servers.

Real-time mirroring of encryption keys.

Real-time mirroring of encryption key configuration and access policies.

Active-Active mirroring between primary and secondary servers.

Must be able to deploy on multiple platforms (HSM, VMware, Cloud).

Full and automatic key mirroring between cloud, virtual, and hardware key servers.

HSM hardware redundancy including network interface, redundant power supplies, and mirrored hot-swappable RAID disk drives.

Automatic secure backup of data encryption keys and key encryption keys.

Ensure you meet industry standards, today and tomorrow.

Dedicated, non-shared key management to meet data security compliance requirements.

MORE READING

WHITE PAPER:
INDUSTRY MUST-HAVES FOR EFFECTIVE ENCRYPTION KEY MANAGEMENT
CLOUD MIGRATION IS NOW IN FULL SWING FOR organizations large and small. The benefits for migrating to the cloud are clear. Reduction in cost for computing power and storage, leverage of converged infrastructure, reduction of IT administrative costs, on-demand scalability, and many other benefits will continue the rapid migration to cloud platforms. As cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and IBM SoftLayer mature we can expect the pace of cloud migration to accelerate.

While cloud service providers are providing some encryption key management capabilities, this area will continue to be a challenge. The question of who has control of the encryption keys (key custody) and the shared resources of multi-tenant cloud service providers are headaches for organizations migrating to the cloud. The emergence of the European General Data Protection Regulations, and the increased aggressiveness of law enforcement and national intelligence agencies also increase the concerns about who has access to encryption keys. The ability to exclusively manage encryption keys and deny access to the cloud service provider or any other third-party will be crucial to a good cloud key management strategy and end-customer trust. The attempt by governments and law enforcement agencies to access encrypted data through access to encryption keys will make this issue far more difficult moving forward.

Unfortunately most cloud service providers have not adopted common industry standards for encryption key management. This results in the inability of customers to easily migrate from one cloud platform to another resulting in cloud service provider lock-in. Given the rapid evolution of cloud computing and the infancy of cloud computing, customers will have to work hard to avoid this lock-in, especially in the area of encryption key management. This is unlikely to change in the near future.

TAKE AWAYS:

Avoid hardware-only encryption key management solutions prior to cloud migration. Make sure your key management vendor has a clear strategy for cloud migration.

Ensure that your encryption key management solution runs natively in cloud, virtual and hardware platforms.

Ensure that your encryption key management solution provides you with exclusive management of and access to encryption keys. Neither your cloud service provider nor your encryption key management vendor should have administrative or management access to keys. Backdoor access through common keys or key management code is unacceptable.

Avoid cloud service provider lock-in to proprietary key management services. The cloud is still in its infancy and retaining your ability to choose and migrate between cloud platforms is important.

CHRISTOPHE KEREBEL My Twitter: @chriskere

CHRISTOPHE KEREBEL My Twitter: @chriskere

CHRISTOPHE KEREBEL My Twitter: @chriskere

CHRISTOPHE KEREBEL My Twitter: @chriskere
LARGE AND SMALL ENTERPRISES WILL continue to grow their virtualization footprints at the same time that they are looking to migrate applications to the cloud. The cost reductions provided by the market leader VMware will ensure that the VMware customer base will continue to consolidate applications and servers on their virtualization technology and that they will continue to be a powerful player in the IT infrastructure space for many years.

While VMware is the dominant technology provider for virtualization, we will continue to see Microsoft invest in their footprint with Hyper-V, OpenStack, and other virtualization technologies. We expect that all of the virtualization solution providers will attempt to define a clear path to the cloud based on their technologies. VMware is already moving in this direction with their vCloud Air initiative, and Microsoft uses Hyper-V as the foundation for the Azure cloud.

Encryption key management solutions that only run in hardware, or that only run on cloud platforms, present substantial obstacles for businesses. The rich set of management and security tools are not able to work effectively with solutions that are outside the virtualization boundary. Custom-key management vendors vary greatly in their ability to support the range of deployments from traditional IT data center, to virtualized platforms, to the cloud. Organizations will continue to struggle with key management across these environments.

“Encryption key management solutions that only run in hardware, or that only run on cloud platforms, present substantial obstacles for businesses.”

**TAKE AWAYS:**

Encryption key management solutions should be able to run as fully native virtual machines in a VMware or Hyper-V environment.

Encryption key management solutions should be compatible with security and management functions of the virtual platform.

To maintain maximum business flexibility, deploy a key management solution that works well in virtual, cloud, and traditional hardware platforms.

Look for key management solutions that carry industry security certifications such as PCI Data Security Standard (PCI DSS), etc.
LAST YEAR WE PREDICTED THAT THERE WOULD be continued consolidation in the key management vendor space, and we really got this one right. With the Thales acquisition of Gemalto (and SafeNet), many of the mainline encryption key management solutions are now under one roof.

As with any consolidation I believe this will have negative impacts on the competitive landscape and on innovation in the key management space. The lack of competition almost always has a negative impact on cost for organizations.

Encryption key management vendors are being absorbed into larger organizations and this trend will likely continue. The public relations around such mergers and acquisitions is always accompanied with glowing prognostications and happy talk. Unfortunately, as often happens with any merger, key management vendors may experience disruption in their organizations as a result of a merger or acquisition. A key management solution may not be strategically important to an acquirer and this can result in disinvestment in the solution negatively impacting customer support. Key management is a part of an organization’s critical infrastructure and these changes can be disruptive.

Organizations can work to minimize the potential impact of key management vendor consolidation by understanding the vendor’s organizational structure, corporate history, and financial basis. Venture backed organizations can be expected to experience an exit through a merger, acquisition, or public offering which may reduce their product focus. Vendors with solutions that are not strategically important to their product mix can also experience change and disruption. Using care in key management vendor selection may be one of the most important efforts you can make. This will be a continuing challenge in the years ahead.

Unfortunately, a merger or acquisition is followed by a lack of investment and innovation in key management products. This is at a time when the tech industry as a whole is undergoing radical changes. Organizations must work to understand a vendor’s commitment to their key management product and look carefully at product roadmaps.

TAKE AWAYS:

Understand your key management vendor’s equity foundation and the likelihood of a merger or acquisition. If the key management vendor is largely funded by venture capital it is almost certain that the company will experience a merger or acquisition event.

Understand your key management vendor’s management team. Have key employees been with the company for a longer period of time? This is one good indicator of organizational stability.
VENDOR CUSTOMER SUPPORT IS AN ONGOING CONCERN

AS MENTIONED PREVIOUSLY, ENCRYPTION
key management vendors continue to be absorbed into larger organizations and this trend will likely continue. Unfortunately, as can happen with any merger, key management vendors may experience disruption in their organizations as a result of a merger or acquisition. This can directly affect the customer support organization and your ability to get timely and reliable technical support for your encryption key management solution. Deteriorating customer support can put your organization at risk. Key management solutions are a part of your critical infrastructure and proper customer support is crucial to operational resilience.

Another side effect of reduced or under-funded customer support is the inability of your organization to expand and invest in new applications and systems. These impacts on customer support may not present short-term problems, but can impair long-term resilience and growth flexibility. Many organizations will continue to experience inadequate customer support from key management vendors.

TAKE AWAYS:

Understand the customer support organization of your key management vendor. Does the vendor demonstrate a strong investment in customer support? Is there adequate management of the customer support team?

Review the Service Level Agreement (SLA) provided by your key management vendor. Be sure you understand the expected response times provided by the vendor customer support team.

How do other organizations experience customer support from your key management vendor? Be sure to talk to reference accounts who use the key management product and who have interacted with the vendor’s customer support team.

“Deteriorating customer support can put your organization at risk. Key management solutions are a part of your critical infrastructure and proper customer support is crucial to operational resilience.”
KEY MANAGEMENT AS A SERVICE

KEY MANAGEMENT AS A SERVICE HAS NOT gotten the traction it needs. Cloud service providers (Amazon Web Services, Azure, Google) have remained fairly static in this area with little additional innovation. Low end key management requirements are very cost effective, but costs get out of control as the number of keys increases. Encryption key management that is not fully under the control of the cloud service provider has been the exception to the cloud service model, but this is about to change. Key-Management-as-a-Service (KMaaS) will be offered by independent Software-as-a-Service providers who will leverage independent key management applications in a shared cloud environment. These solutions will be low-cost, multi-tenant solutions with a self-service model, and will offer enterprise options and migration paths for dedicated key management and key management that is deployed outside of the cloud platform.

KMaaS offerings will finally provide smaller organizations access to validated technologies and to technologies that are based on industry standards such as the Key Management Interoperability Protocol (KMIP). Due to the cost of traditional key management solutions, smaller organizations and startups have been excluded from access to professional key management. The good news is that new KMaaS offerings will bring low-cost solutions in within the reach of small and midsize organizations.

TAKE AWAYS:

KMaaS solutions should be based on FIPS 140-2 compliant key management solutions.

KMaaS solutions should provide a path to both dedicated key management, and to key management hosted outside of the cloud service provider platform.

KMaaS solutions should provide a self-service model for allocating and managing the service.

KMaaS solutions should be independent of cloud service provider administrative access.

WHITE PAPER:

ENCRYPTION KEY MANAGEMENT IN MULTI-PLATFORM ENVIRONMENTS

DOWNLOAD

CHRISTOPHE KEREBEL My Twitter : @chriskere
WE GOT THIS ONE RIGHT LAST YEAR, AND IT continues to be accurate. With MongoDB’s adoption of KMIP as the key management interface in their Enterprise database, KMIP is proving its worth as an industry standard. The standard is maintained by the OASIS standards group and has gained wide acceptance by the encryption key management vendor community. The first version of the standard was published in 2010 and the standard continues to undergo active development. KMIP describes both how key management servers and key management clients interoperate.

This last year has been a watershed in the adoption of the KMIP standard by client-side applications. From storage to Big Data to VMware to ISV applications, KMIP has quickly become the standard method for integrating with enterprise key management systems.

Unfortunately, the KMIP standard does not address server management functions such as server deployment and activation, network interface configuration, certificate generation and distribution, system logging, backup and restore and so forth. This aspect of encryption key management will continue to be a challenge. Some vendors are making an effort to address the need for server management, but there is no standard for server management.

Additionally, initial client-side implementations of KMIP are often inadequate from a business recovery point of view. Many client-side applications using KMIP do not implement hot failover to a secondary key server. This can present a challenge for customers who depend on highly available applications. The use of load balancers and similar technologies can mitigate this weakness to some extent. We expect to see client-side applications evolve over time.

**TAKE AWAYS:**

Encryption key management solutions should be KMIP compliant to insure future compatibility with evolving client-side applications.

Where vendors are not providing ready-to-use applications or software development kits (SDKs) give preference to solutions that implement KMIP.

Virtual storage solutions will continue gain more traction; be sure to insist on the implementation of KMIP for all virtual storage and SAN solutions.
ENCRYPTION AND KEY MANAGEMENT SHOULD move from an IT project to an integrated and seamless part of the IT infrastructure. Organizations need to be able to deploy encryption with ready-to-use infrastructure so that encryption ceases to be a barrier. In order to accomplish this encryption and key management solutions must be embedded in the IT infrastructure and enabled by policy. Key management solutions must implement the automation infrastructure that enables this type of deployment. All aspects of the provisioning of an encryption key server from network configuration, system logging, user administration, generation and distribution of credentials, key mirroring, backup and restore, and encryption key management must become API driven through standard web services.

Unfortunately, standards bodies and vendors have been slow to address this critical aspect of key management. While there is some movement to define some aspects of encryption key management through web services or add-on solutions like Chef and Microsoft Desired State Configurations (DSC) support, the network and services aspects of key managers have not been adequately addressed. This will continue to make it difficult to move key management into the realm of seamless and invisible critical infrastructure.

TAKE AWAYS:

Ask your key management vendor how they implement APIs for server configuration, deployment and management.

Understand the key management vendor’s roadmap and plans for key management automation.

Ask the key management vendor for examples of customers using their Web services features.

Understand any vendor licensing restrictions for installing management utilities.

PODCAST: Key Management Guidelines

DOWNLOAD
THERE IS NO SINGLE SOURCE FOR BEST OF BREED SECURITY

Understandably, customers long for a single vendor who can solve all of their security needs. Currently the process of deploying best of breed security involves working with multiple vendors whose products do not interoperate. It means spending a lot of IT resources managing a large variety of vendor products and services. While there are a handful of larger vendors attempting to provide a complete set of products, their marketing language does not match reality and there is no indication that it will for some time to come. This continues to be a challenge.

Smart organizations will identify best of breed applications that are easy to use, and make the resource investments needed to acquire and manage these solutions.

TAKE AWAYS:

- Always try to deploy the best of breed security solutions and understand that this means dealing with multiple vendors.
- Prioritize your security needs according to risk, and tackle the highest priority items first.
- Understand and empower your IT organizations to acquire and deploy the best solutions. It is always more cost effective to prevent a problem than remediate it after the fact.

“While there are a handful of larger vendors attempting to provide a complete set of products, their marketing language does not match reality and there is no indication that it will for some time to come. This continues to be a challenge.”
CYBER INSURANCE IS EVOLVING TO LIMIT LIABILITY PAYMENTS

WHILE ENCRYPTION IS ONE OF THE MOST effective ways to protect sensitive information, organizations large and small continue to fail to get this critical control right. The most common failure is the failure to protect information at all. When cyber-criminals gain access to sensitive data they often find that it is not encrypted or protected. That means they only need to steal the data in order to reap the rewards. It is likely that unprotected data will remain a strong cause of sensitive data loss. Not much has changed in this area over 2016.

For organizations that use encryption, the most common cause of a data loss or compliance audit failure is the failure to protect encryption keys. When keys are stored on the same server, or hard-coded in applications, or protected with weak passwords, cyber-criminals find it easy to decrypt the data. Failing to protect the encryption key continues to be a common cause of security audit failures, and demonstrates a lack of commitment to reasonable security controls.

"Failing to protect the encryption key continues to be a common cause of security audit failures, and demonstrates a lack of commitment to reasonable security controls."

These two encryption failures will continue to plague organizations in 2016. New European Union data protection regulations are now coming into effect that will drive adoption of encryption and proper key management. The EU regulations are very specific in the mandate for data protection and proper key management, including business continuity requirements for key management. The United States is lagging in this type of strong mandate, but actions like the recent State of California guidance from the Attorney General Kamala Harris will rapidly change this dynamic. It is likely that we will continue to see the lack of encryption or poor key management continuing to plague organizations for at least the near term.

TAKE AWAYS:

Encryption is a crucial element of your security strategy. Be sure that all sensitive information is protected with strong encryption such as AES.

Encryption keys should never be stored on the server where your sensitive data resides.

Be sure you have the right technology to store and protect encryption keys.

Encryption key management is crucial to your encryption strategy. Make sure that encryption keys are protected by key management systems that meet industry standards.
WE’VE SEEN SOME IMPROVEMENT IN THE SaaS space related to encryption key management. SaaS vendors have caught on that larger enterprises expect the best in the way of security best practices, and newer SaaS offerings are doing better in the area of key management. No SaaS vendor wants to lose a deal with a global company because of poor security practices. Some SaaS solution providers clearly understand the need for encryption, segmentation of data, and encryption key management and there has been improvements, but most are focused on meeting customer business needs and the competitive environment that security takes a back seat to market share. This is not a good situation for organizations that depend on SaaS vendors for their security posture. Non-existent, weak, or poorly implemented encryption and key management put organizations at risk. Almost all SaaS solutions avoid any responsibility (liability) for a failure of their security implementation. This will continue to be the case for most SaaS offerings where license agreements clearly avoid responsibility for common and avoidable security failures.

TAKE AWAYS:

Be sure to understand your SaaS vendor’s implementation of encryption and key management.

Is your data logically or physically segmented from other customers? Is encryption implemented with proper key management?

Do you have the option of managing encryption keys outside of the cloud?

What responsibility does the SaaS provider accept for securing your data? What responsibility do you have?

Does the SaaS solution meet compliance regulations such as PCI-DSS, HIPAA, FFIEC, and GDPR? What evidence do that have for meeting compliance from third party security auditors?
TOWNSEND SECURITY CREATES DATA PRIVACY
solutions that help organizations meet evolving com-
pliance requirements and mitigate the risk of data
breaches and cyber-attacks. Over 3,000 companies
worldwide trust Townsend Security’s NIST and FIPS
140-2 compliant solutions to meet the encryption and
key management requirements in PCI DSS, HIPAA/HI-
TECH, FISMA, GLBA/FFIEC, SOX, and other regulatory
compliance requirements.

CONTACT TOWNSEND SECURITY
www.townsendsecurity.com
@townsendsecure

724 Columbia Street NW, Suite 400
Olympia, WA 98501

360.359.4400