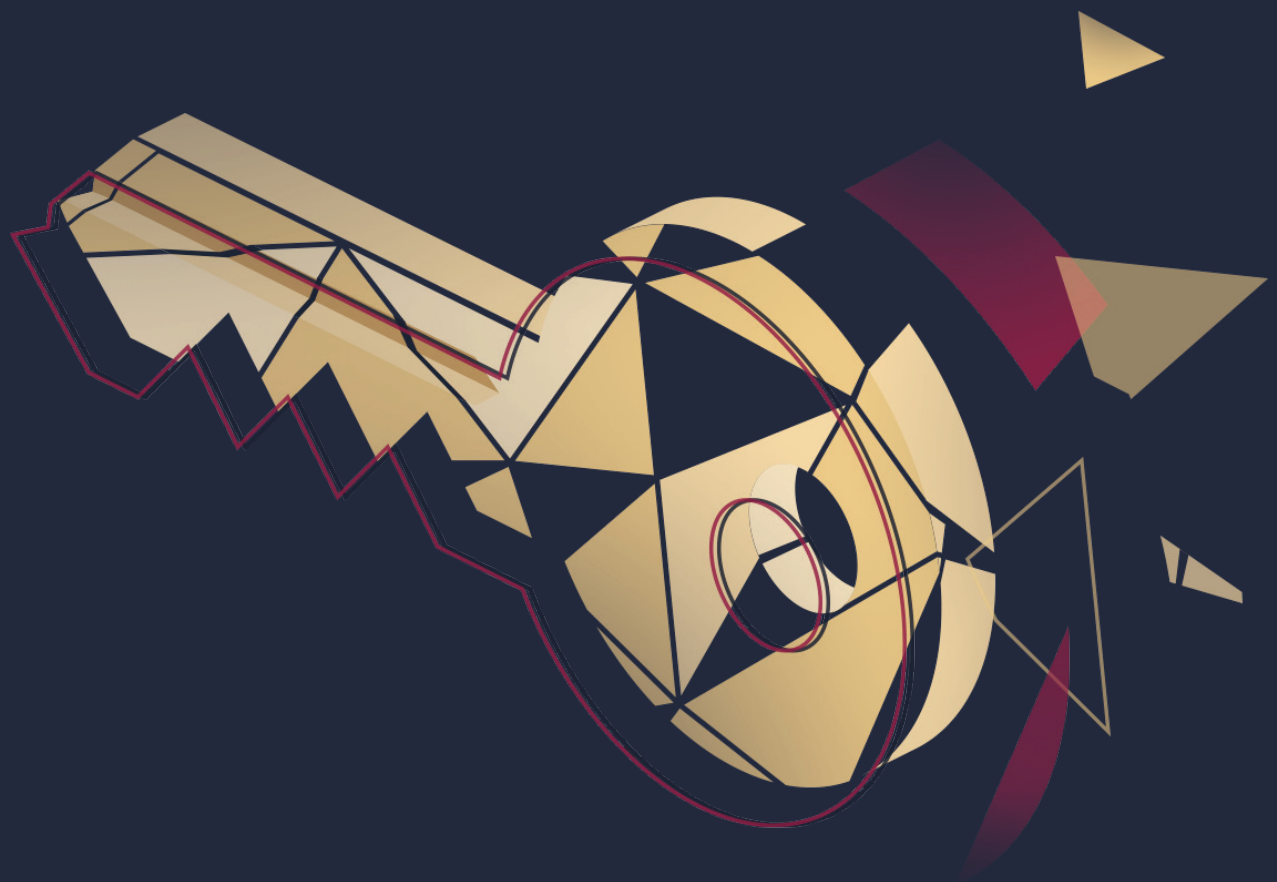
Cryptographic Key Management Trends in 2020

A joint report from the Cyber Security Competency Group (CSCG) and Unbound Tech



UNBOUND
(MATH OVER MATTER)

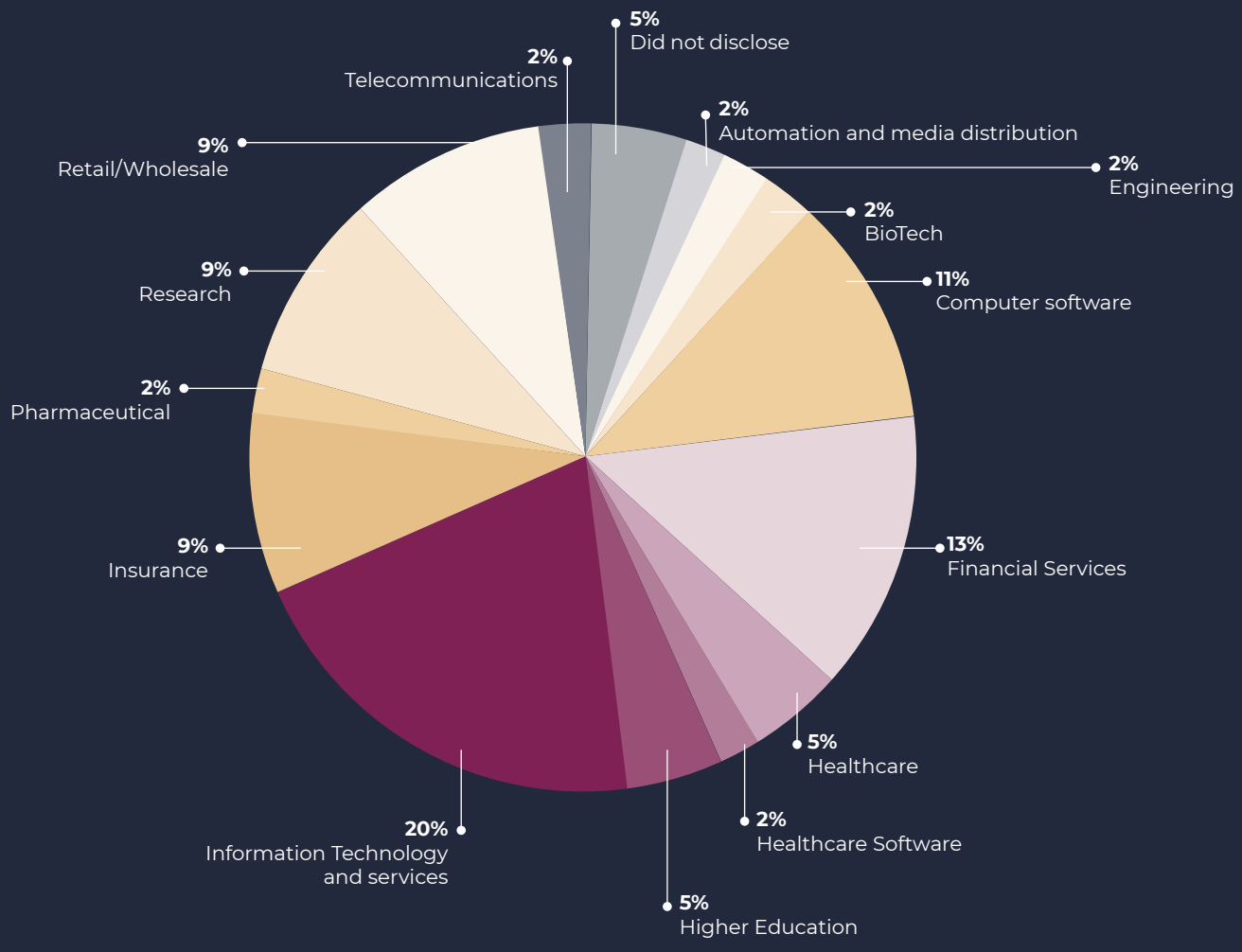
Introduction

In September 2019, Unbound Tech surveyed 500 members of the Cyber Security Competency Group (CSCG), a group of cybersecurity professionals (analysts, engineers, and architects) from different industries across North America. The survey addressed cryptographic key management and certificate management practices.

Respondents hailed from a variety of industries, illustrated below. The top 3 industries represented in this report are Information Technology and Services (20%), Financial Services (11%), and Computer Software (11%).

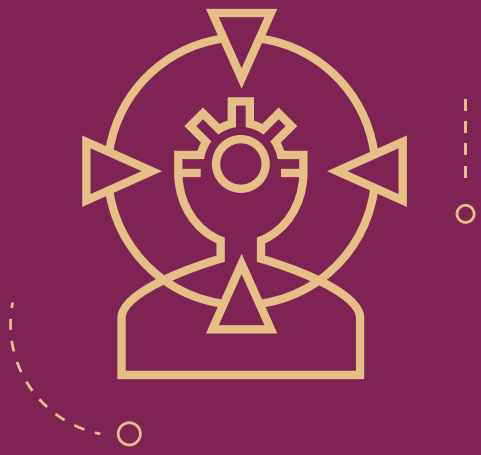
What they all had in common, however, is that their organizations manage cryptographic keys. How they do it - and how well -- will be addressed in this report.

Survey Respondents - By Industry



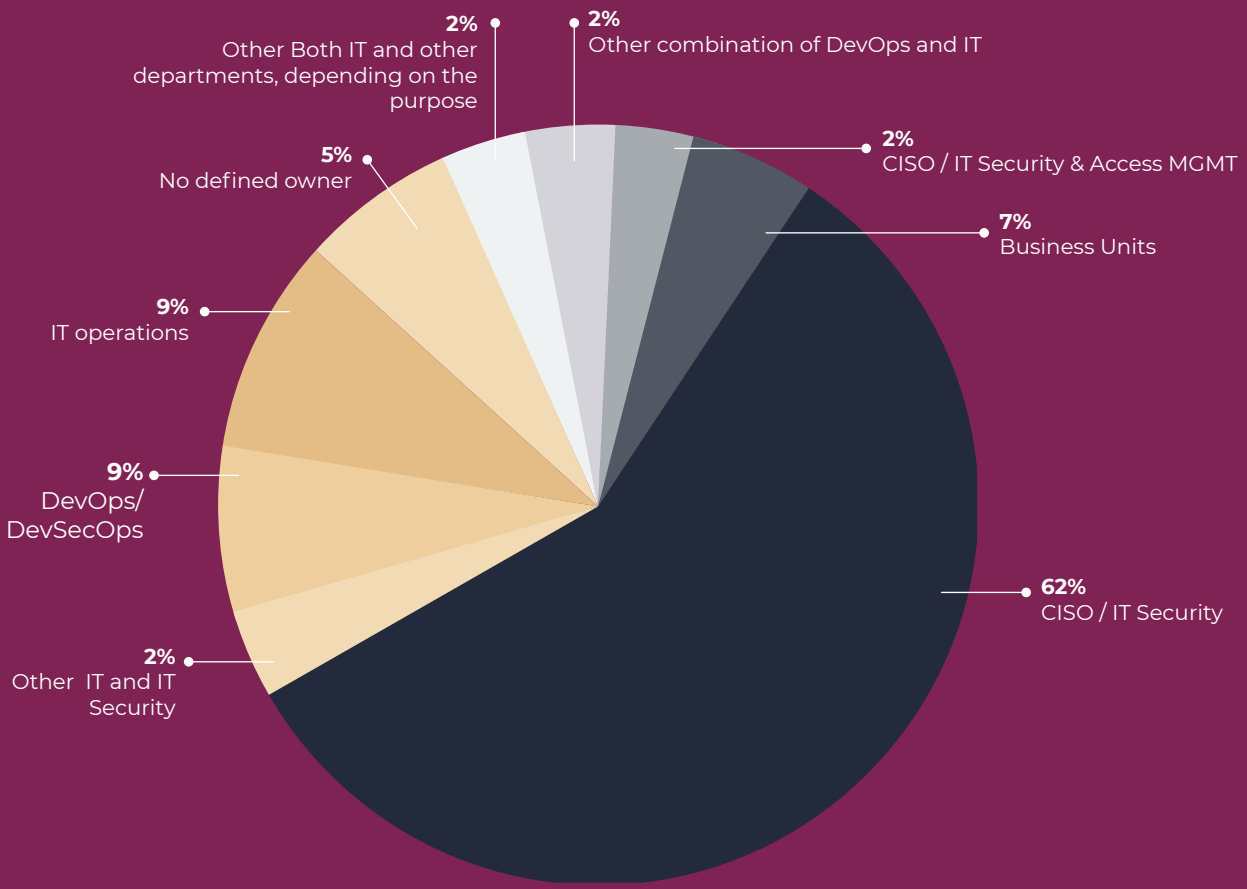
Who oversees key management?

Key management generally remains in the hands of the traditional stakeholders: departments dedicated to information technology (IT) and/or security. In the survey conducted in 2019, 62% of respondents stated that a Chief Information Security Officer (CISO) and/or the IT department of their organization is responsible for key management and administration within their organization.



Of the remainder, 9% of respondents stated that IT operations were responsible for key management; 7% responded that business units were responsible for key management; 9% of respondents stated that DevOps or DevSecOps are responsible for key management (especially in Computer Software companies); 6% responded “other”; and 5% stated that there was no defined owner of their company’s key management.

Key Management Owner - By Department



Key management challenges by industry

Key management remains a challenge for most industries – especially for regulated and risk averse industries like BFSI (banking, financial services & insurance) and healthcare, and in much lesser extent to tech-savvy industries like IT and computer software. This report examines those challenges and reveals which trends may be industry - specific.

The report found that the less tech-savvy the organization, the more difficult it was for them to manage their keys.

- 66% of respondents stated that was a “big” or “medium” challenge for their enterprise
- Of the 21% who cited lack of key visibility as a “big” challenge, the majority hailed from the Financial Services, Healthcare & Insurance industries
- 45% of respondents said it was a “medium challenge”
- The only industries which stated it was a “small” problem or non-issue were Computer Software and IT professionals - some 29% of respondents

Even IT professionals struggle with visibility of keys kept in the cloud.

- 57% of respondents stated it was a “big” or “medium” challenge – including IT professionals
- 12% of respondents stated it was a “big” challenge- particularly Financial Services (18%) and Retail (18%) professionals

Managing keys across multiple clouds remains a challenge as well, with 68% stating it was a “big” or “medium” challenge, and 24% of respondents stating that it was a “big” challenge (particularly from Financial Services, Insurance and IT).

Multiple clouds present issues of compatibility; keys created on one cloud are not accessible from another (or compatible), and vice versa, creating multiple silos with limited visibility and segmented auditability.

While keeping keys on multiple clouds may be the result of utilizing different features from different cloud service providers (CSPs), reverse compatibility issues lead to operational and organizational problems vis-à-vis those keys’ maintenance in the long-term.

Integrating KM with new services or operations presents its own difficulties. 52% stated it was a “big” or “medium” challenge.

Cryptography is one of the foundational tools that organizations can use to protect sensitive data wherever it resides. Key management in all organizations has become a critical issue, as the number of applications – and endpoints – has skyrocketed with the digital transformation.

While respondents were fairly evenly distributed across all industries, Insurance, Financial and Healthcare services particularly cited integration as a major pain point. One notable exception is IT and computer software – where the majority of respondents from those industries rated KM integration as a “Medium”-level problem.

The same could be said of adapting or scaling KM to meet enterprise needs – wherein 45% stated it's a "big" or "medium" challenge, and 14% stated it's a "Big" challenge.

As the data that needs to be protected increases in an organization, the number of encryption keys that need to be maintained increases.

This is compounded by the fact that:

- Organizations are more distributed, with multiple data centers and even more applications and services that span them.
- Monolithic applications are giving way to increasingly distributed, and sometimes short-lived, microservices such that organizations must manage keys at wider scale without compromising security.
- Market demand to offer services and products that require increasing agility, scalability and performance—therefore making it difficult and complex to manage individual keys at the enterprise scale.

Who's using which KM solution?

Many organizations don't have a KM system – and of those that do, some use one or more cloud KM[1] due to their multi cloud presence, in addition to on-prem KM and cryptographic key storage systems (e.g. multiple types of HSMs). Indeed, best practices for key management dictate that key management systems should be present throughout the enterprise, including both on-prem and in cloud applications.

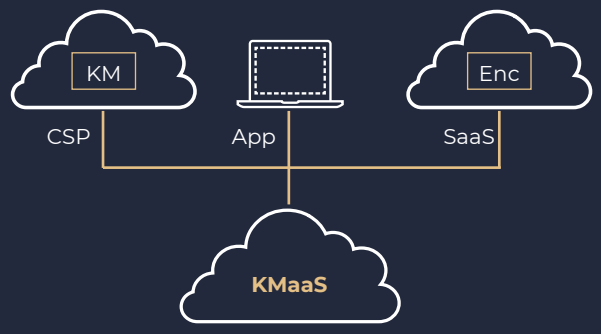
Enterprises may choose to handle this in different ways, including one or more of the following:

- Key management as a service (KMaaS)
- On-prem enterprise key management system
- Cloud key management system (deployed on-prem)
- CSP KM

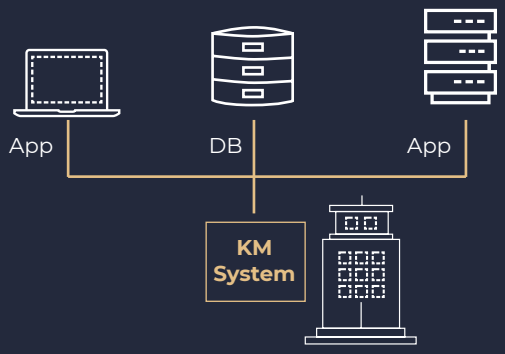
With different cloud service providers and on-premises sites across multiple geographic locations, and their respective key management systems, enterprises lack the ability to manage their entire cryptographic arsenal across all sites, all existing HSMs and all workloads on-prem and in multi-cloud from a single pane of glass. There is an absence of automatic key sync between different sites and workloads which results in key management in silos.

The diagram below illustrates some common key management structures.

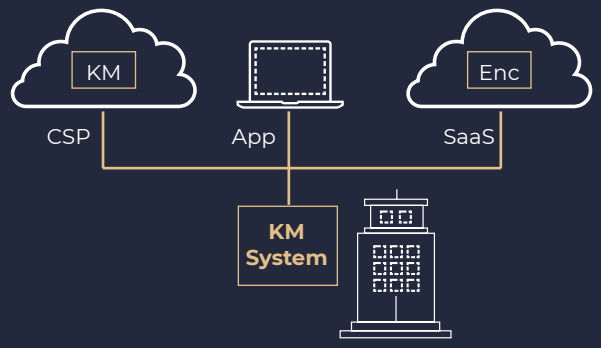
KMaaS



On-prem Enterprise KM System



Cloud KM System (deployed on-prem)



CSP KM

Ideally, cryptographic keys would be managed, visible, and able to be administrated via a single pane of glass. Here's what happens in reality:

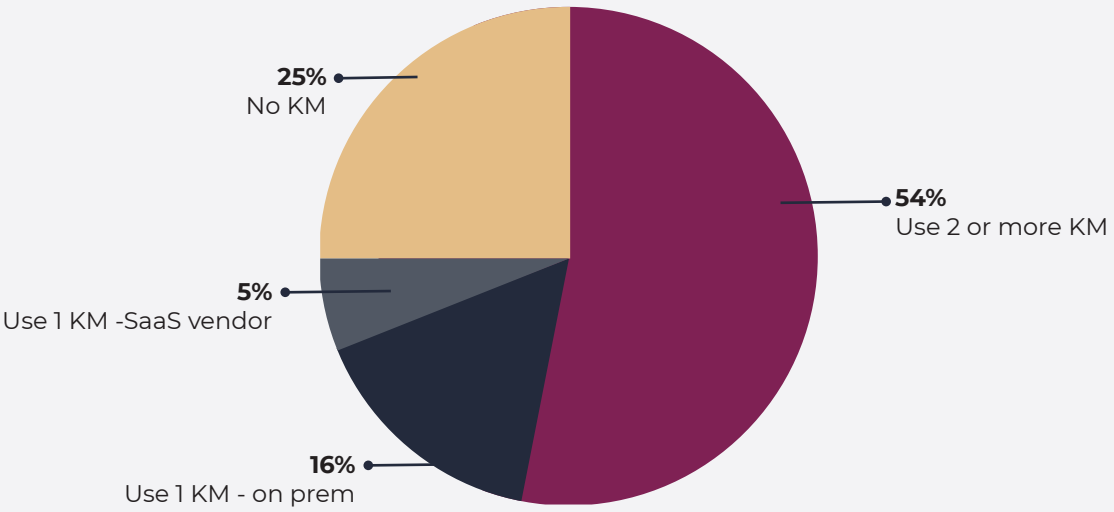
54% of respondents are using 2 or more key management systems or services, whether on-prem or in the cloud. Of these, most respondents hailed from the Financial Services, IT, Insurance, and Healthcare industries. This is logical because these market verticals use a large number of applications (homegrown or 3rd party), have extensive interfaces with customers and suppliers, and are part of a very large eco-system.

21% of respondents said their organizations use one key management system – 16% on-prem and just 5% via SaaS vendors.

25% of respondents said their organizations are not using a key management solutions at all, including most respondents from the computer software industry.

(1) Key Management Service of a cloud service provider, such as AWS KMS, Azure Key Vault, GCP KMS, etc.

Percentage of Respondents using a KM System

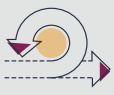


What are the most important parameters for choosing a KM solution?

Operational efficiency is key for KM clients. Respondents were asked which of the following parameters are the most important in choosing a key management system -- here were the results:

38% prioritize a comprehensive set of integrations and APIs
Highest industries represented: IT (18%) and FIS (18%)

19% cited a "proven security level" - and 40% of respondents who cited security as the primary parameter in their decision-making worked in the IT industry



32% prioritize ease of administration.
Highest industries represented: FIS, Insurance, Research, Retail (14% each)

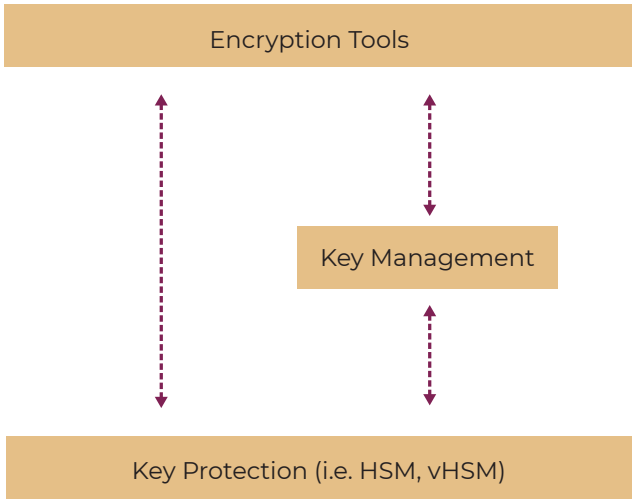
6% chose a strong deployment track record

Encryption

When asked about encryption practices in their organization, results are varied. 59% of respondents are using encryption products from multiple vendors – primarily in IT, Insurance and Financial Services. 39% of respondents say their companies use the same vendor for key management and encryption-- and most of the respondents in this category stem from the Financial sector, IT, or Research.

The cryptographical world is built on three main pillars: encryption, key management and key protection. Vendors that develop all three of these product lines deliberately created a vendor lock-in mechanism in such a way that their encryption tools can be integrated only with their own key management and HSMs. The vendor lock-in doesn't stop there: KM providers each require a specific HSM to integrate with, which then require specific encryption tools per system, creating closed eco-systems. The following figure depicts the cryptographic stack.

We discovered that FIS, Insurance, and IT companies using multiple KM systems are likely using multiple encryption products due to vendor lock-in. Spreading multiple keys across multiple platforms or clouds means building entirely disparate silos – and creating even more of a mess for key management across the board.



Conclusion

Key management, in all of its aspects, continues to be a challenge for the burgeoning enterprise – especially in the midst of the digital transformation. Ease of use, integration between APIs and various on-prem and cloud systems, and full transparency and visibility plague most organizations – *especially* those in the Financial, Insurance, Retail and Healthcare sectors.

Challenges repeatedly arise in these sectors due to a conflation of industry-specific factors. Each of these industries deals with a large number of clients; each involves a host of regulatory compliance considerations, both external and internal; each involves a variety of teams and technologies. Challenges in the IT and CS industries are likely due to the wide range of tools, technologies, and frameworks teams use to deploy security measures and/or develop code – and the restrictions and pitfalls of using several cloud-based services, KM, encryption tools, etc.

Overall, enterprises struggle to manage their entire cryptographic arsenal across all sites and systems. The result is wasted expenditure on duplicate key management products, wasted time and efficiency lost in the switch between tools, problematic visibility- and, ultimately, compliance and audit issues. We recommend that each of these industries look closely at the possibility of streamlining their security and KM services – if possible, in a single pane of glass.

Unbound Tech
www.unboundtech.com
contact@unboundtech.com

Follow Us

UNBOUND
(MATH OVER MATTER)