IBM Security Services
White Paper

Protecting your company’s most critical information

Not all data is created equal

Compliance is important. But does it mean your most critical data is truly protected?

Ensuring your data is compliant can be a fairly straightforward task. Your IT team works their way through the checklist, and stays out of trouble with lawyers and regulatory agencies. There's value to that. But true data protection is more than regulatory compliance. In fact, even if you're compliant, your organization could still be at risk unless you strategically identify and protect your most valuable data.

Traditionally, you've been presented with IT security metrics—sometimes reassuring, other times alarming. But simply reviewing IT security metrics is not meaningful in and of itself. As an executive, you don't evaluate issues in siloes. Instead, you excel at assessing issues in the broader context of your organizational operations. In other words, technical security data and metrics lack value unless viewed through the lens of business risk.

When you're presented with IT security metrics, your question is: What does this mean for my business? And ultimately, what data should I be most concerned with? *The point is, not all data deserves equal protection*. A more effective approach is to understand:

- Which data is most critical (also known as "crown jewels")?
- Where does that data reside?
- How is it exposed to security risks?
- What potential impact would a security breach to this data have on your organization?
- What are the appropriate steps to take based on the data's criticality?

Ideally, this information should be offered in a business-consumable, highly visual presentation—one that clearly delineates business impact and risk exposure in a concise, actionable format.

News alerts on your phone? In 2016, they were often about the latest hack attack. Russia was accused of interfering in the US elections. One of the world's largest internet companies reported a sizable breach. According to *The Economist*, the World Anti-Doping Agency, a major bank in Bangladesh and a large US government agency were also hacked.[1] 2017 has been rocky, with a global ransomware attack impacting organizations from China to Britain in May.[2] In fact, mobile ransomware has risen by over 250 percent during the first few months of 2017.[3]

But your organization doesn't have to make international headlines to feel the pain. Incredibly, many small to medium cyberattacks essentially go unreported in the media while still wreaking havoc on targeted organizations. As a result, cybersecurity is attracting greater focus in the C-suite, with security metrics receiving increased scrutiny.

Conversations

- Your organization has passed all required security compliance audits — what are the gaps between checking those boxes and truly protecting your data?
- What is the difference between treating security as a set-it-and-forget-it proposition versus an evolving challenge?

The “aha” moment for a leading insurance company

Do your security specialists know where your customers’ personally identifiable information (PII) is stored? For one major insurance company, the answer was no — as revealed by an internal audit. The reaction was immediate, with the board of directors and executive team realizing they needed to monitor and protect that data to safeguard their business.

The vice president of enterprise data management was tasked with discovering where the critical data was located, protecting it, and giving the executive team the right business-consumable insights to take action to protect her business and mitigate risk. The company turned to IBM Data Risk Manager for help.

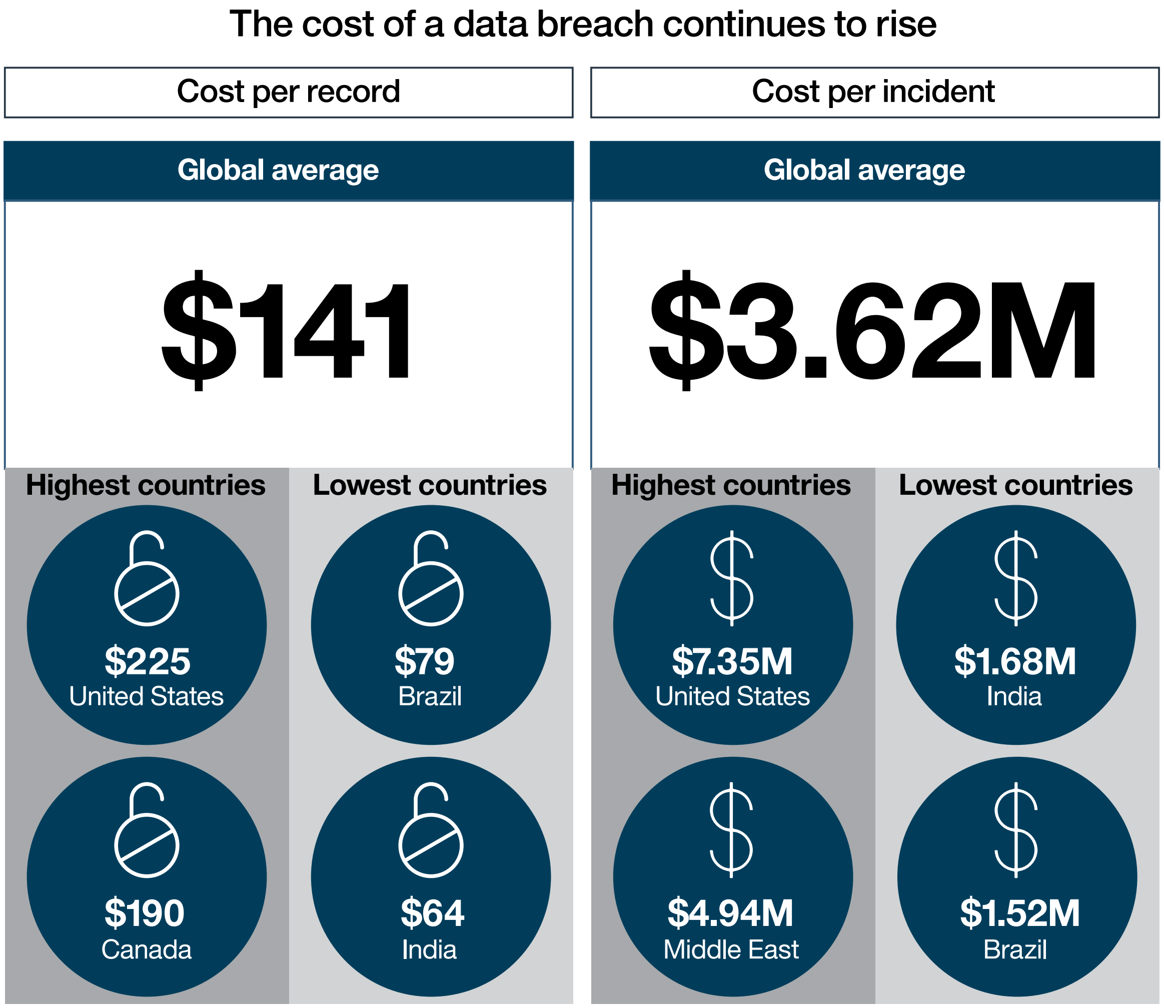
The customer PII was the most critical data element. In interactive reports, Data Risk Manager technology identified this as a crown jewel — indicated by a crown icon. The team could easily see that PII was contained in 17 locations and had 6 alerts indicating policy violations. To determine if an investigation was warranted, they quickly identified consumers, stakeholders, application owners, associated business partner data flows, and the infrastructure and applications that had access to the data.

The solution enabled the IT team to scan reports to find false positives, as well as validate and perform classifications. Then, the team analyzed data and identified potential risks across the environment. The interactive dashboard, or control center, presented the information in a business-friendly format, providing a snapshot of information that helped determine data-related business risk.

The aha moment was when it got visual. The interactive Data Risk Manager visual control center enabled everyone from tech leads to the board of directors to more easily understand critical information — even from mobile devices and tablets. This clarity allowed the team to take targeted actions to dramatically improve their security posture.

Using technology to assess, communicate and alleviate business risk: four questions

Security incidents are frequent and damaging. As shown in Figure 1, the average cost per record breached globally is USD141, and the average cost per incident globally is USD3.62 million.[4]



The cost of a data breach continues to rise

Cost per record		Cost per incident	
Global average		Global average	
$141		$3.62M	
Highest countries	Lowest countries	Highest countries	Lowest countries
$225 United States	$79 Brazil	$7.35M United States	$1.68M India
$190 Canada	$64 India	$4.94M Middle East	$1.52M Brazil

Source: 2017 Cost of Data Breach Study: Global Analysis, by Ponemon Institute
Currencies converted to U.S. dollars

Figure 1: Costs and impacts of data breaches continue to pose challenges.

As you re-evaluate your own organization's data scenarios, you'll need to implement a strategy that accurately assesses and communicates risks—and protects mission-critical data. And as an executive, you'll want the ability to visualize your technical risk scenario within a broader business context. *It's the potential business impact that's a catalyst for action—not the security threat in and of itself.*

Here are four "big picture" questions to keep in mind.

1. Not all data is created equal: What are the crown jewels of your data?

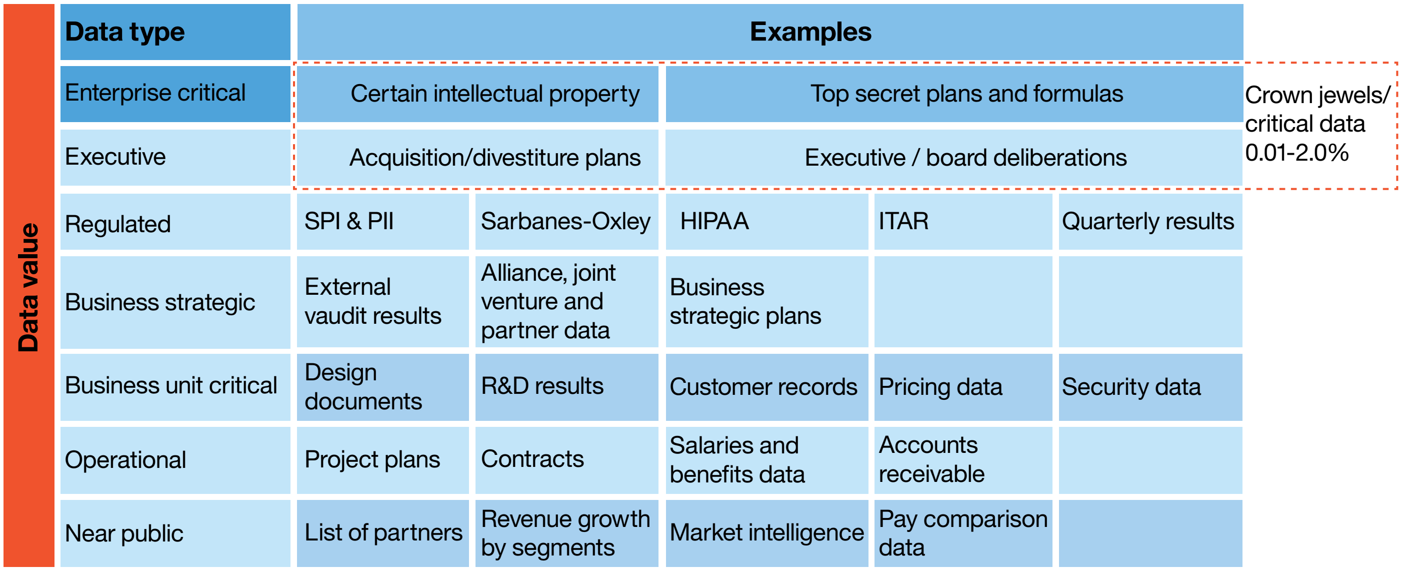
A very small percentage of your overall data can represent almost three-quarters of your organization's market value. Critical data—also known as crown jewels—is the data that ensures your business survival and success.

This mission-critical data could be customer information, intellectual property, product designs, financial information and more. While typically only .01 percent to 2.0 percent of total sensitive data volume is considered crown jewel data, the stakes are high. It can be helpful to consider your data type on a spectrum, with enterprise-critical and executive data at maximum criticality and operational and near-public information at lower value and lower risk. (See Figure 2.) Crown jewel data usually belongs to one of the following categories:

- Enterprise critical, which can include intellectual property like confidential plans, patent development and industry-transforming innovations, as well as customer information
- Executive, which can include executive deliberations, behind-the-scenes decisions and financial forecasts
- Regulated, which can include information that must comply with Sarbanes-Oxley, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other guidelines

If stolen, this information's exposure could not only put you out of compliance—your organization could be debilitated if top-secret plans and strategies are leaked.

Crown jewel data is usually found in the top two or three data categories.



Data value	Data type	Examples					
	Enterprise critical	Certain intellectual property		Top secret plans and formulas			Crown jewels/ critical data 0.01-2.0%
	Executive	Acquisition/divestiture plans		Executive / board deliberations			
	Regulated	SPI & PII	Sarbanes-Oxley	HIPAA	ITAR	Quarterly results	
	Business strategic	External vaudit results	Alliance, joint venture and partner data	Business strategic plans			
	Business unit critical	Design documents	R&D results	Customer records	Pricing data	Security data	
	Operational	Project plans	Contracts	Salaries and benefits data	Accounts receivable		
	Near public	List of partners	Revenue growth by segments	Market intelligence	Pay comparison data		

Figure 2: Crown jewel data is of high value to an organization and is usually found in the top two or three data categories.

Conversations

- What data would have significant business impact if it were compromised?
- How do you protect these "crown jewels"?

2. Abstractions get lost in the noise. How can you assess and summarize specific security risks to your crown jewels?

A company may generate, acquire, process, share and store vast qualities of sensitive data, and try to protect it all—but not very well. With a clear understanding of what comprises critical data, or crown jewels, you can determine what devices and machines should be used to store it, and whether the information is structured or unstructured. The goal is to provide awareness and visibility to critical information assets, how they are protected and who or what has access to them—then assess the risk of loss or exposure.

But how do you accomplish this assessment and identification? You'll need a way to:

- Discover and classify sensitive information
- Analyze incidents and threat vectors from security information and event management (SIEM)-type products
- Analyze reports from infrastructure governance and management products
- Perform advanced analytics to identify sensitive assets subject to potential compromise

Ideally, you can capture a complete view (processes, procedure, compliance, ownership and more) of sensitive data. From that vantage point, it is much easier to understand specific, high-value business-sensitive data at risk from internal or external threats.

Conversations

- How do you currently prioritize and assess your crown jewel data for risk of loss?
- How do you authorize individuals who access this business-critical data? Who are the business owners?
- Where is this business-critical data located? Do these storage repositories contain any security vulnerabilities?

3. Focus where it counts: How do you analyze critical data security concerns against business objectives?

As an executive, you may often be presented with detailed IT metrics around data security. Yet most of these metrics are seldom useful to the C-suite unless they place potential risks within a business context. How can you be certain that data security risks are presented to you and your C-suite colleagues in the most constructive format?

Your organization will need a solution that helps you visualize, understand and manage risks associated with the protection of sensitive data—at a glance. The solution should integrate with data protection, SIEM capabilities and infrastructure governance products to map potential threats against sensitive business assets. And, *visualizing* risks to sensitive assets across departments and business functions can clarify potential impacts.

Just like the insurance organization we visited earlier, your organization's aha moment could come from a dashboard-type solution that communicates value and context. The dashboard serves as a visual tool that enables the right conversations across the C-suite, IT, security and line-of-business (LOB) teams to improve business processes and manage risks.

The end result? *Actionable* information from a *visual* command center—and solid support for a comprehensive critical data protection plan.

Conversations

- How are you currently communicating security and data metrics to your C-suite?
- How can you gain better visibility into potential risks around data security?

4. In command: Taking action to protect your critical data

Your next step is to work with your IT staff to develop a comprehensive risk mitigation plan. And security exposures clearly outlined in a visual format help garner the support you need from your C-suite peers to move that plan forward. Specifically, you'll want the risk mitigation plan to:

- Account for all of the data's business owners and likely users, and every control point of the data through its lifecycle
- Prioritize your assets, using an identify-discover-analyze-rank-classify process
- Enable as much access and sharing as is required for an effective enterprise operation—but within the context of your data governance program, processes and controls
- Encompass an ongoing and continuously evolving program–not a short-term exercise. This helps ensure enhanced controls, the continuous monitoring of assets, and a repeatable process for discovery and classification

What you don't know can *hurt you. Master your risk with a command center that lets your organization see and address data-related business risk.*

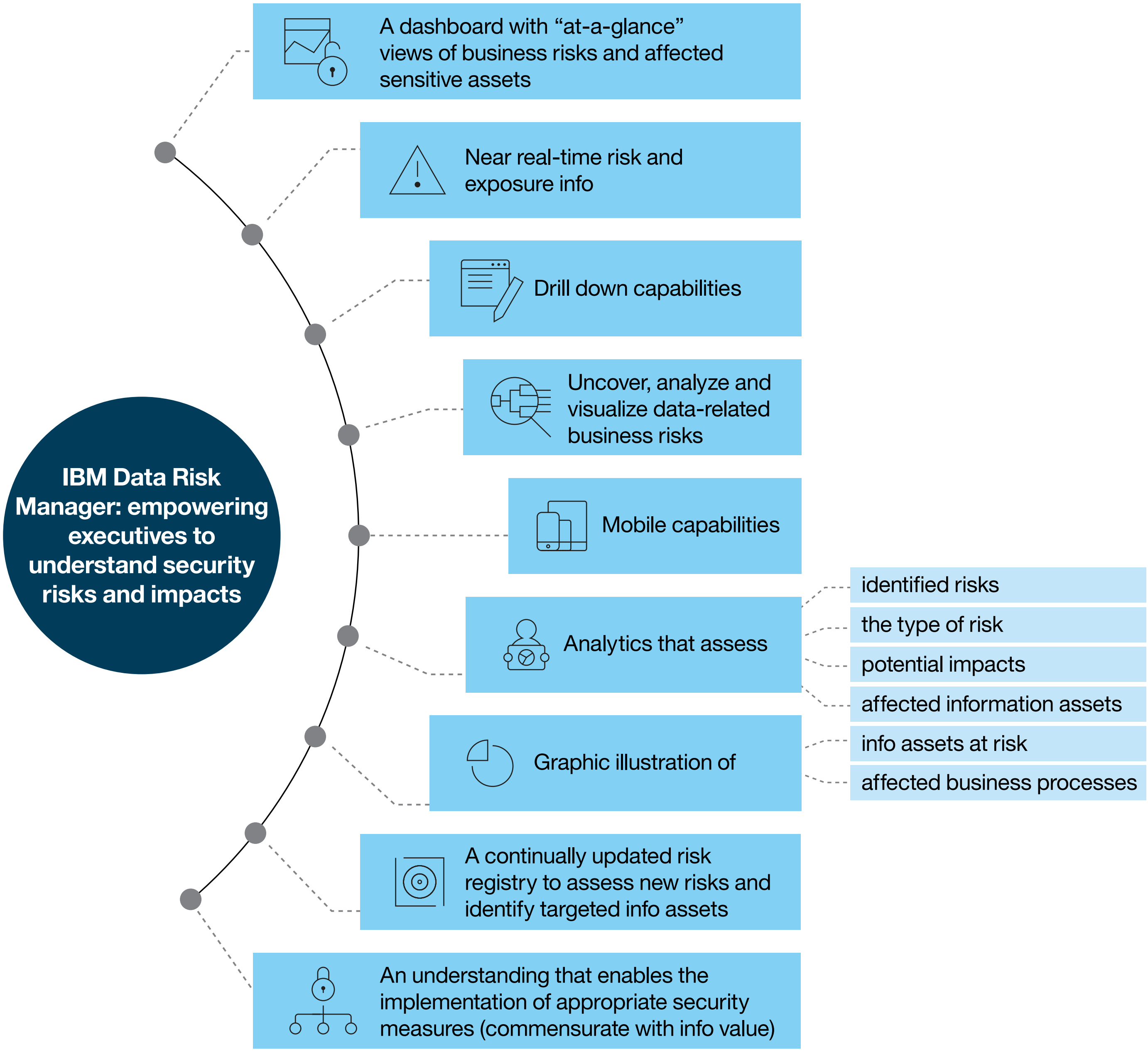
Conversations

- Your IT team says you have security controls in place such as data loss prevention (DLP). How exactly does that protect your data? What are additional exposures?
- With a vast amount of data in your organization and exponential growth of mobile and cloud, where do you even start in terms of developing a plan?

Why IBM?

Conversations about your critical data security—and your resulting strategies—are among the most important you'll have. With one of the most advanced and integrated portfolios of enterprise security products and services, IBM® Security can help. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations; monitors 20 billion security events per day in more than 130 countries; and holds more than 3,000 security patents. IBM has hired approximately 1,900 security specialists since 2015.

In February 2017, IBM acquired Agile 3 Solutions, LLC. to provide dynamic views of data-related business risk to executives. IBM Data Risk Manager leverages these capabilities to help uncover, analyze, and visualize risks, so that the right action can be taken to proactively protect the business. IBM Data and Application Security Services offer delivery expertise to use Data Risk Manager as an integration platform to correlate threats, vulnerabilities, controls and business attributes with the value of the information asset. This information is then used to calculate a risk score that highlights the parts of the business that are at risk. (See Figure 3.) Learn more at **ibm.com**/us-en/marketplace/data-risk-manager.



IBM Data Risk Manager: empowering executives to understand security risks and impacts
A dashboard with "at-a-glance" views of business risks and affected sensitive assets
Near real-time risk and exposure info
Drill down capabilities
Uncover, analyze and visualize data-related business risks
Mobile capabilities
Analytics that assess
identified risks
the type of risk
potential impacts
affected information assets
Graphic illustration of
info assets at risk
affected business processes
A continually updated risk registry to assess new risks and identify targeted info assets
An understanding that enables the implementation of appropriate security measures (commensurate with info value)

Figure 3: IBM Data Risk Manager places security risks in the context of business impact.

For more information

Ready to learn more about how IBM Security and IBM Data Risk Manager can help you identify and manage security risks? Check out our website, view a video demo and get in touch with a representative — all by visiting **ibm.com**/us-en/marketplace/data-risk-manager

References

1 "Incentives need to change for firms to take cyber-security more seriously." The Economist. Dec. 20, 2016. (www.economist.com/news/leaders/21712138-software-developers-and-computer-makers-do-not-necessarily-suffer-when-their-products-go)

2 Scott, Mark and Nick Wingfield. "Hacking Attack Has Security Experts Scrambling to Contain Fallout." New York Times. May 13, 2017 (www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html?_r=0)

3 Cuthbertson, Anthony. "Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest." Newsweek. May 23, 2017. (www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034)

4 Ponemon Institute. "2017 Cost of Data Breach Study: Global Analysis." Ponemon Institute, sponsored by IBM. June 2017. https://www.ibm.com/security/data-breach/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
November 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.