RAZ-LEE

EBOOK

Ensuring your IBM i is compliant with government and industry regulations

APRIL 2020

Table of Contents

Introduction

Government and industry regulations, including GDPR, PCI-DSS, Sarbanes-Oxley (SOX), and HIPAA, stipulate measures that companies must take to ensure proper data security and monitoring. These regulations are mandatory, and lack of compliance can trigger severe penalties, from fines to legislative actions.

PCI-DSS, SOX and HIPAA compliance requirements have significantly impacted the IT staff of business, financial and healthcare companies, presenting major challenges to both public and private enterprises. In May 25, 2018 GDPR went into effect. GDPR is unprecedented in its attempt to create a harmonized data protection framework able to meet the technological challenges of the modern age. It affects all organizations, companies and entities worldwide that process the personal data of individuals within the EU. The impact is experienced in all aspects of an organization from IT, legal, marketing, customer service, to even HR. Now the California Consumer Privacy Act (CCPA) has been added to the mix effective January 1, 2020.

CCPA is the first consumer privacy act in the United States. It is designed to protect the data privacy rights of citizens living in California. California is the only state that provides its citizens with GDPR like protection against any entity that does business within it.

This e-book provides an overview of the major regulations and the security and monitoring measures that need to be implemented to comply.

GDPR

The General Data Protection Regulation

Overview

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation that reinforces and binds together information security for all people inside the European Union (EU). It supersedes the European Union Data Protection Directive of 1995 which led to different privacy laws in different European countries. GDPR is intended to protect personal data and establishes how organizations process, store, and ultimately destroy it when the data is no longer required.

The regulation went into effect on May 25, 2018 and affects all organizations, companies and entities worldwide that processes personal data of individuals within the EU. Non-compliance will result in fines of up to EUR 20 million or 4% of the global annual corporate revenue, whichever is greater.

“Non-compliance will result in fines of up to EUR 20 million or 4% of the global annual corporate revenue, whichever is greater.”

GDPR Security Objectives

- Establish data privacy as a fundamental right.
- Protect personal data for anyone based in the EU or handling the personal data of anyone in the EU.
- Protect this personal data via processes, technology and automation.
- Place direct legal obligations on data processors.
- Establish responsibilities of companies based in the EU or providing goods or services to anyone in the EU.
- Establish a baseline for data protection based on GDPR requirements.
- Elaborate on data protection principles: not only encryption but also assessment, prevention, detection controls.

Key Changes

CONSENT

The Regulation requires more active consent to support lawful processing of personal data; wherever consent is required for data to be processed, consent must be explicit, rather than implied.

GOVERNANCE

Organizations have increased responsibility and accountability on how they control and process personal data. This would require a proactive approach by organizations to develop adequate data management processes.

TRANSPARENCY

Organizations have increased transparency obligations; privacy notices will need to include much more detailed information.

DATA PORTABILITY

Organizations must ensure data subjects can easily transfer their data files from one service provider to another.

RIGHT TO BE FORGOTTEN

The GDPR consecrates the “right to be forgotten”, allowing data subjects the right to require a controller to delete data files relating to them if there are no legitimate grounds for retaining it.

DATA PROTECTION OFFICER

Companies have to appoint a Data Protection Officer when they are, for example, processing sensitive data. The DPO will report to the highest level of management.

Impact on Companies and Data Processors

DATA SECURITY MEASURES

Companies have direct responsibility to ensure appropriate data security measures are adopted when processing data. Previously this responsibility sat exclusively with the customer (controller), but will now need to be actively managed jointly in co-operation with the customer on a mutually agreed basis.

RECORD KEEPING

Companies must maintain a full record of all 'processing operations' which they carry out on behalf of their customer involving the processing of personal data. This means keeping an up-to-date register of services being performed on each category of customer originating data.

NOTIFICATION OF DATA BREACH

Companies will be required to notify the customer (controller) 'without undue delay' as soon as it becomes aware of a data breach involving loss of personal data. Customers are likely to expand on this in contractual arrangements, to meet their own obligations to notify regulators within 72 hours of a breach.

DATA SUBJECT RIGHTS

The GDPR gives individuals the right to request a copy of their personal data, to seek erasure, modification or portability of their data and (in certain cases) withdraw consent/object to certain types of processing activity. EU based organizations will expect systems and processes offered by companies to be designed to help comply with these requirements. Companies should build supporting functionality into systems.

SUPPLY CHAIN MANAGEMENT

Customers will be required to conduct more robust risk assessments before engaging third party providers to process data. They will apply more robust contract protections and conduct regular audits. Companies should be prepared to respond positively to this evolving regime, especially during tender processes and contract negotiations to mitigate risk and create a competitive advantage.

Mapping Key GDPR Requirements

iSecurity can help organizations accelerate compliance for IBM i servers with several GDPR obligations.

	ARTICLE	HIGHLIGHTS	DATA SECURITY REQUIREMENTS	iSecurity
ASSESS	Data protection impact assessment *Art. 35 and 84	Assessment of the purpose, scope and risk associated with processing personal data	Inventory of personal data across organization, access rights to data, and risk associated with that access	Data Discovery Assessment Authority Inspector Compliance Evaluator
PROTECT	Security of processing *Art. 5, 6, 25, 28, 29, 32, 64 and 83	Implement appropriate technical and organization security controls to protect personal data against accidental or unlawful loss, destruction, alteration, access or disclosure	▪ Pseudonymization and encryption ▪ Ongoing protection ▪ Regular testing and verification	Anti-Ransomware Encryption Firewall Anti-Virus Authority on Demand
DETECT	Data breach notification *Art. 30, 33 and 34	72 hour notification to Data Protection Authority following discovery of data breach, and notification to affected individuals	Breach report that includes: ▪ what happened ▪ numbers of affected individual ▪ what data was breached	Audit AP-Journal Capture SIEM / DAM Support Change Tracker

CCPA

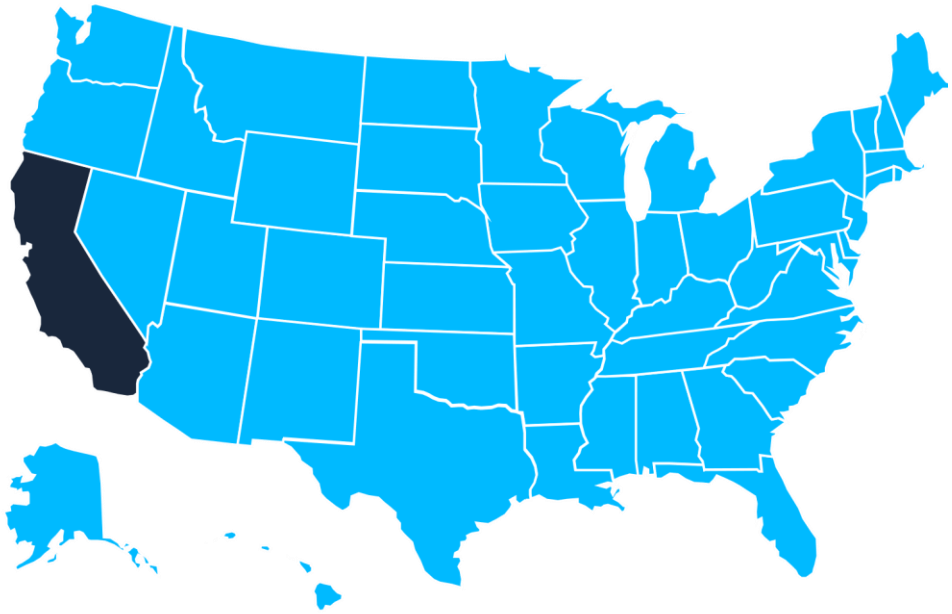
The California Consumer Privacy Act

Overview

The California Consumer Privacy Act (CCPA) is a regulation that sets new privacy rights and consumer protection for California residents. CCPA was signed into law on June 28, 2018 and amends Part 4 of Division 3 of the California Civil Code.

The CCPA provides California residents with the right to:

- Know what personal data is being collected about them.
- Know whether their personal data is sold or disclosed and to whom.
- Say no to the sale of personal data.
- Access their personal data.
- Request a business to delete any personal information about a consumer collected from that consumer.
- Not be discriminated against for exercising their privacy rights.



Companies Required to Comply

The CCPA applies to any business, including any for-profit entity doing business in California that collects consumers' personal data and satisfies at least one of the following thresholds:

- Has annual gross revenues in excess of $25 million;
- Buys or sells the personal information of 50,000 or more consumers or households; or
- Earns more than half of its annual revenue from selling consumers' personal information.

Impact on Companies

DISCLOSURE OBLIGATIONS

Companies are required to inform consumers about their rights under CCPA, what categories of information they collect, how that information will be used, and what information is shared with third parties. Companies cannot discriminate against consumers because they exercised the rights granted in the bill.

CONSUMER RIGHTS

Companies must put in place processes to comply with consumer requests to view all the information the company has about them, delete that information and opt out of the sale of their information. Companies must have processes in place to confirm the identity of the consumer making the request.

OPT-OUT MECHANISMS

Companies must place a link titled “Do Not Sell My Personal Information” visibly on their website

AUTHORIZATION OF MINORS

The sale of children’s data requires express opt-in consent. If the child is between 13 and 16 years old, express opt-in consent can only be collected directly from the child. If the child is under 13 years of age, express opt-in consent must be obtained from the parents or legal guardian.

CCPA & iSecurity

The regulation went into effect on January 1, 2020 and affects all organizations, companies and entities worldwide that do business in California.

The California Attorney General is required to publish the regulations for compliance by July 2, 2020. Non-compliance will result in civil penalties of up to USD 7,500 per violation.

iSecurity can help organizations implement data security measures to comply with CCPA.

> “Non-compliance will result in civil penalties of up to USD 7,500 per violation.”

PCI-DSS

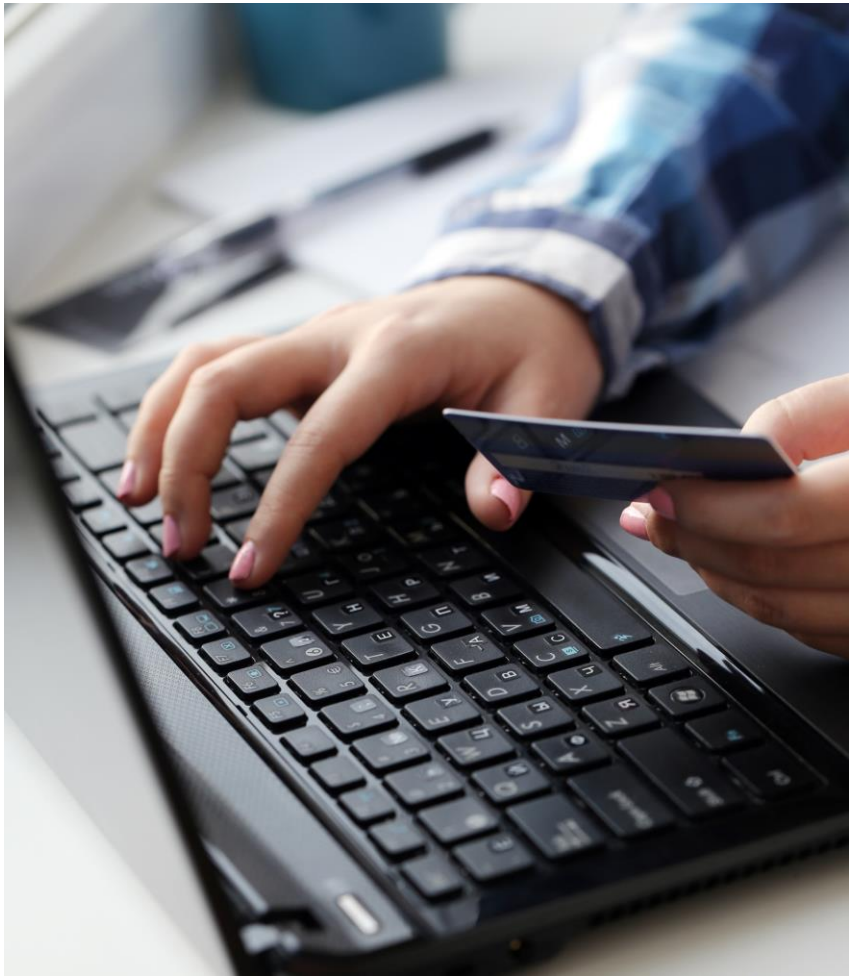
The Payment Card Industry Data Security Standard

Overview

The Payment Card Industry Data Security Standard (PCI-DSS) is a worldwide information security standard assembled in 2004 by the Payment Card Industry Security Standards Council. The standard was created to help organizations that process card payments prevent credit card fraud through increased controls on data. The standard applies to all organizations which hold, process, or pass credit card information.

A merchant (in all instances) failing to comply with any part of the regulation might be severely fined by the PCI Security Standard Council, by up to $500,000 per incident. At the end of the day, the company is responsible for how it manages its data, and, regardless of the size of the organization, its compliance must be assessed on a regular basis.

Compliance is mandated by the payment card brands and not by the PCI Security Standards Council.



Complying with PCI-DSS

PCI-DSS consists of 12 requirements within six categories that cover best security practices. Here is a summary of these requirements, focusing on the relevant items to IBM i security.

- Build and Maintain a Secure Network
  - Requirement 1: Configure a Firewall
  - Requirement 2: Default Passwords and Parameters
- Protect Cardholder Data
  - Requirement 3: Protect Stored Data
  - Requirement 4: Encrypt Transmission
- Maintain a Vulnerability Management Program
  - Requirement 5: Anti-Virus
  - Requirement 6: Secure Systems and Applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict Access
  - Requirement 8: Assign Unique ID
  - Requirement 9: Restrict Physical Access
- Regularly Monitor and Test Networks
  - Requirement 10: Monitor Access
  - Requirement 11: Test Security
- Maintain an Information Security Policy
  - Requirement 12: Maintain a Policy

Mapping Key PCI-DSS Requirements

iSecurity facilitates compliance with all the PCI-DSS articles that are relevant to IBM i Security.

	ARTICLE	DATA SECURITY REQUIREMENTS	iSecurity
ASSESS	Manage user accounts and proactive vulnerability scans *Art. 8.1, 11.2	Implement procedures to ensure access rights to data, and run internal and external network vulnerability scans.	Assessment Compliance Evaluator Visualizer
PROTECT	Access control and data security *Art. 1.3, 2.3, 3.3, 3.4, 3.5, 5.1, 5.2, 7.1, 7.2, 8.2, 8.3, 8.4, 8.5, 11.4	Implement appropriate technical policies and procedures that ▪ protect user accounts ▪ control access to data ▪ secure Primary Account Number (PAN) ▪ protect cardholder data against accidental or unlawful loss, destruction, alteration, access or disclosure	Anti-Ransomware Encryption Firewall Anti-Virus Authority on Demand 2 Factor Authentication
DETECT	Security surveillance and reports *Art. 6.3, 10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 11.3, 11.5, 12.9	Implement automated audit trials of user activity and file integrity monitoring software, review for security compromise, and alert and resolve unauthorized activity.	Audit AP-Journal Capture SIEM / DAM Support

SOX

The Sarbanes-Oxley Act

Overview

The Sarbanes-Oxley Act, widely known as SOX, is a United States federal law enacted in 2002. SOX relates to the review of dated legislative audit requirements to protect investors by improving the accuracy and reliability of corporate disclosures, establishing a public company accounting oversight board, corporate responsibility, auditor independence, and enhanced financial disclosure.

A corporate officer who does not comply or submits an inaccurate certification is subject to a fine of up to $1 million and ten years in prison, even if done unintentionally. If a wrong certification was submitted purposely, the fine can be up to $5 million and twenty years in prison.

SOX Mandates & Requirements

SOX contains 11 titles that describe specific mandates and requirements for financial reporting:

- Public Company Accounting Oversight Board (PCAOB)
- Auditor Independence
- Corporate Responsibility
- Enhanced Financial Disclosures
- Analyst Conflicts of Interest
- Commission Resources and Authority
- Studies and Reports
- Corporate and Criminal Fraud Accountability
- White Collar Crime Penalty Enhancement
- Corporate Tax Returns
- Corporate Fraud Accountability

> “A corporate officer who does not comply or submits an inaccurate certification is subject to a fine up to $1 million and ten years in prison, even if done unintentionally.”

SOX Compliance with COBIT

COBIT, or the Control Objectives for Information and related Technology, is an arrangement of best practices for IT administration made by the Information Systems Audit and Control Association and the IT Governance Institute (ITGI) in 1996.

COBIT provides an arrangement of for the most part acknowledged measures, pointers, and processes intended to maximize the benefits from the use of information technology and develop appropriate IT governance and control in corporate enterprises.

COBIT is a recommended framework for assessing SOX compliance. iSecurity facilitates compliance with all COBIT requirements relevant to IBM i Security: Articles 5.1-5.20.

Mapping Key SOX Requirements

	SECTION	DATA SECURITY REQUIREMENTS	iSecurity
ASSESS	Manage data classification, Security and user accounts *DS 5.1, 5.4 and 5.8	Implement procedures to ensure that security measures, data across organization, access rights to data, and risk associated with that access are in line with business requirements	Assessment Compliance Evaluator Visualizer
PROTECT	Access control and data security *DS 5.2, 5.3, 5.9, 5.16, 5.17, 5.18, 5.19, 5.20	Implement appropriate technical policies and procedures that ▪ control access to data ▪ secure the transmission of sensitive data ▪ protect data against accidental or unlawful loss, destruction, alteration, access or disclosure	Anti-Ransomware Encryption Firewall Anti-Virus Authority on Demand
DETECT	Security surveillance and reports *DS 5.7, 5.10	Log all security activity and ensure that it is reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity.	Audit AP-Journal Capture SIEM / DAM Support

HIPAA

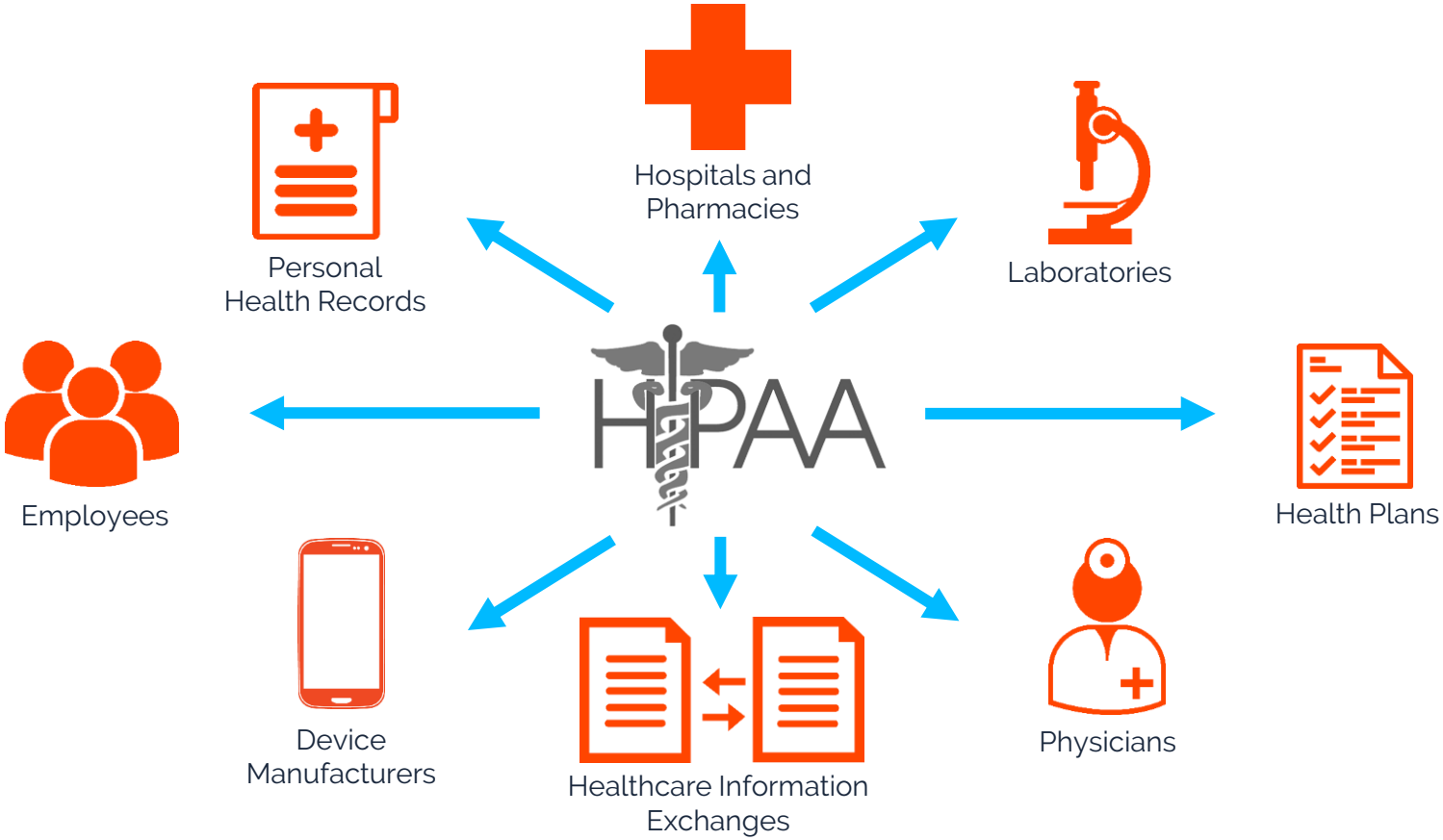
The Health Insurance Portability and Accountability Act

Overview

The Health Insurance Portability and Accountability Act (HIPAA) enacted by the U.S. Congress in 1996, is a group of regulations that work to combat waste, fraud, and abuse in health care delivery and health insurance. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, addresses the security and privacy of health data.

The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision.

Covered Entities and Business Associates



HIPAA Requirements for Enterprises

- Institute a required level of security for health information, including limiting disclosures of information to the minimum required for the activity.
- Designate a privacy officer and contact person.
- Establish privacy and disclosure policies to comply with HIPAA.
- Train employees on privacy policies.
- Establish sanctions for employees who violate privacy policies.
- Establish administrative systems in relation to the health information that can respond to complaints, respond to requests for corrections of health information by a patient, accept requests not to disclose for certain purposes, and track disclosures of health information.
- Issue a privacy notice to patients concerning the use and disclosure of their protected health information.
- Establish a process through a Review Board (or privacy board) for a HIPAA review of research protocols.
- As a health care provider, include consent for disclosures for treatment, payment, and health care operations in treatment consent form (optional).

> "The penalties for noncompliance are based on the level of negligence . . . with a maximum penalty of $1.5 million per year for violations of an identical provision."

Mapping Key HIPAA Requirements

iSecurity facilitates compliance with all the HIPAA articles which are relevant to IBM i security.

	SECTION	DATA SECURITY REQUIREMENTS	iSecurity
ASSESS	Audit controls and integrity *Sec. 164.312(b) and 164.312(c)(1)	Implement necessary policies and measures that record and examine activity in information systems to protect them from improper alteration and destruction	Assessment Compliance Evaluator Visualizer
PROTECT	Access control and data security *Sec. 164.312(a)(1), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(a)(2)(vi), 164.312(d), 164.312(e)(1), and 164.312(e)(2)(ii)	Implement appropriate technical policies and procedures to control access to electronic protected health information and security controls to protect data against accidental or unlawful loss, destruction, alteration, access or disclosure	Anti-Ransomware Encryption Firewall Anti-Virus Authority on Demand
DETECT	Emergency *Sec. 164.312(a)(2)(i), 164.312(c)(2) and 164.312(e)(2)(i)	Implement unique user identification for identifying and tracking user identity, mechanisms to corroborate that data has not been altered or destroyed, and integrity controls to ensure timely detection	Audit AP-Journal Capture SIEM / DAM Support

Assess, Protect, & Detect with iSecurity

Raz-Lee's iSecurity solutions assist IBM i companies in attaining maximum compliance with government and industry regulations. By providing ready-made tools tailored to meet the requirements of these regulations, iSecurity enables companies to effortlessly achieve data safety and compliance.

About Raz-Lee Security

Raz-Lee Security, headquartered in Nanuet, New York, is a leading independent cybersecurity and compliance solutions provider for IBM's IBM i (AS/400) midrange computers. With more than 35 years of expertise and customers in over 40 countries, Raz-Lee's flagship iSecurity suite guards organizations against insider threat and unauthorized external access to business-critical information hosted on their IBM i. The company continues to develop and market cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

www.razlee.com