SOLUTION SPOTLIGHT

NAVEX GLOBAL®

Major Health Insurer Manages Vendor Risk with NAVEX Global's GRC Platform

SOLUTION

LP LOCKPATH®
INTEGRATED RISK MANAGEMENT

EP NE PT RR LP

HIGHLIGHTS

COMPANY

Major Health Insurer

CHALLENGE

Comply with HIPAA data security requirements and other regulations and frameworks

SOLUTION

Third-Party Risk Management

RESULTS

Insight into vendor operations, lower risk of HIPAA fines and monthly metric reporting for CISO

Comprehensive Vendor Risk Management

- Create and manage vendor profiles
- Conduct vendor assessments efficiently
- Link vendors to policies, risks, controls and more
- Communicate and collaborate with third parties
- Conduct performance reviews
- Perform ongoing monitoring

Manual Processes Prove Inefficient for Managing Vendor Risk in Today's Regulatory Environment

Like most in the healthcare industry, a major health insurer complies with the Health Insurance Portability and Accountability Act (HIPAA), as well as many other regulations and requirements. A primary HIPAA compliance requirement is assessing vendors regularly, as well as assessing vendors' third parties. Compliance failures can lead to stiff fines.

Previously, the health insurer relied on manual processes for vendor risk management activities like issuing assessments. A manual approach can be suitable for a small business with a handful of vendors, but for a health insurer with HIPAA requirements, it can be risky and error prone. The need for efficiency and accuracy turned the major health insurer into an early adopter of governance, risk management and compliance (GRC) platforms. However, the GRC platform the company chose was overly rigid and required technical expertise to configure. The process of managing vendor risk assessments was so complicated that the risk management team reverted to using manual processes.

With the challenge still present, the health insurer conducted a search for a more advanced GRC platform that offered the functionality to comply with healthcare regulations, required little or no IT assistance and a high degree of user adoption.

NAVEX Global's Advanced Governance, Risk Management & Compliance (GRC) Platform

The health insurer's search for a GRC platform led the company to NAVEX Global's Lockpath, which offers a flexible and scalable solution for integrated risk management and includes the ability to streamline vendor risk assessments.

Lockpath was easy to configure to the health insurer's processes. Since implementation, Lockpath has enhanced the health insurer's ability to identify, analyze, track and report on vendor risks with quick user adoption. Features like drag-and-drop reporting and an intuitive interface made it possible for users to create reports quickly and easily.

A defined process for managing vendor risk

With Lockpath, the health insurer's IT Risk team can enforce its defined vendor risk assessment process. Doing so ensures vendors have the proper security controls in place to meet HIPAA requirements for protecting patient data.

The team assesses vendors by issuing 10-20 questionnaires internally with staff who each represent a segment of the vendor base. Each questionnaire is designed to measure the inherent risk of the vendor based on the classification and volume of data that the vendor accesses, stores, processes or outsources. Of these initial questionnaires that canvas the entire vendor base, any vendors that score and qualify as high inherent risk are required to complete a comprehensive vendor security assessment questionnaire.

Comprehensive questionnaires help the health insurer identify security control gaps that are tracked as findings within Lockpath's risk register. The number of findings, along with the inherent risk score, drive the overall third party risk score as low, medium or high for each vendor. As third parties remediate their findings, their risk score is reduced, which lowers the insurer's overall third party risk.

In addition, Lockpath enables the IT Risk team to map assessment questions to controls within the Health Information Trust Alliance Common Security Framework (HITRUST CSF). This allows the IT Risk team to measure all vendors against a healthcare industry framework that also maps to HIPAA.

Data from completed questionnaires can be formulated as an ongoing report that lists vendors compliant with HIPAA and which ones are not. The information easily produced in Lockpath communicates the overall vendor risk to executive management.

Reporting keeps management informed

With Lockpath, the health insurer has a central repository for all risk data. This data is correlated, analyzed and delivered in management and executive-ready reports with the ability to drill-down to supporting data.

For example, the IT risk manager uses the platform to produce automated monthly metric reports for his CISO. The reports are easily generated every month, and if the CISO requests additional detail, Lockpath simplifies creating a new report with additional data.

Using Lockpath, the health insurer can report on everything from internal IT risks and cybersecurity incidents to IT audit findings and vendor risks.

LOCKPATH®
Integrated Risk Management

Integrated Risk Management

Integrated Risk Management (IRM) is the collection of practices and processes that offer businesses a comprehensive view of how they identify, assess and prioritize risk throughout their organization. Lockpath, a GRC and Integrated Risk Management solution from NAVEX Global, equips users and business leaders to manage risk from the endpoint to the enterprise.

Lockpath's integrated risk management capabilities address eight business use cases:

- » Compliance and policy management
- » Vendor risk management
- » IT risk management
- » Continuous monitoring
- » Business continuity management
- » Operational risk management
- » Audit management
- » Health and safety management

Results: turning risk into opportunity

While HIPAA fines for vendor data breaches capture the headlines, this major health insurer is capturing data on its vendors and managing vendor risk. Efficiencies using Lockpath also afford the IT Risk team more time to perform due diligence, which helps protect the company. Each year, the IT risk manager expands his department's reliance on Lockpath, which now encompasses managing cybersecurity incidents, IT audit and assessment findings. Moving forward, the plan is to continue leveraging Lockpath to engage in more efficient ways of managing risk and compliance.

ABOUT NAVEX GLOBAL

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services. Trusted by more than 14,500 customers, our solutions help organizations manage risk, address complex regulatory compliance requirements and foster an ethical, highly productive workplace culture. For more information, visit www.navexglobal.com.