Deloitte.

Getting started

Becoming a quantified organization

January 2024

Risk and compliance

Automating compliance with internal and external requirements

Risk and compliance

Automating compliance with internal and external requirements

Compliance is expensive for organizations and time consuming and non-engaging for individual workers. Advances in data collection— such as managing access without passwords and or multi factor authentication—can enable organizations to reduce the time and costs of compliance and limit the burden of this work on workers while simultaneously improving the accuracy of these kinds of efforts. Automating compliance work can also enable workers and the organization to pursue higher value tasks and opportunities.

As the cases in this section illustrate, organizations can apply the quantified organization model to a wide variety of risk and compliance issues. Some cases here illustrate opportunities to use data trails to identify insider threats and related risks. Other cases point toward new tools to enable workers to better manage tax compliance challenges using location data. By increasing the security of the customer's personal data, the organization can create shared value at the societal level while complying with regulations and avoiding the associated fines.

While these tools show promise, it is critical to use them in ways that build trust. For instance, despite the widespread use of location data in phones and consumer devices, our survey found that only 23% of workers were comfortable sharing their location data with their employer, while other technologies, such as facial recognition technologies, can create privacy concerns as well as potential challenges related to bias and accuracy.[1] To address these, organizations should consider collecting this data on an opt-in basis when possible while continually auditing these systems to ensure that they are not producing unexpected errors or challenges.

Identifying insider risks by picking signals from passive data

Representative data sources

- Workers' access to sensitive data on custom apps

Representative technology areas

- AI (user behavior analytics)

Shared value creation

Individual level

- Protecting individuals accessing sensitive data for legitimate purposes

Enterprise level

- Threat identification
- Risk mitigation
- Regulatory compliance

Society level

- Increased security of customer's banking data

Use case maturity

Exploratory	Emerging	**Maturing**

Key challenge[2]

A bank wanted to identify sources of insider fraud related to workers accessing sensitive customer data on the bank's custom apps. The bank's legacy fraud detection system provided alerts when workers accessed sensitive customer data but it did not provide context related to data use on these apps.

As a result, the system often generated false positives alerting the threat intelligence team even when workers were accessing or using customer data for legitimate purposes. Some workers needed to access sensitive data for longer periods and the legacy system wasn't sophisticated enough to consider the underlying reasons for accessing this data.

Solution and approach

With the help of a third-party vendor, the bank improved their insider fraud detection program to reduce false positives and accurately identify data misuse by workers. Through past data and AI behavioral analytics, the bank developed baselines about reasonable durations for which workers need to access sensitive data.

The baseline estimates were also layered with additional information about context; access durations and parameters could vary by job descriptions and job levels. The context-based solution alerted the threat intelligence team when a worker accessed sensitive data for a duration longer than the baseline estimates and beyond permitted contexts.

The application also maintained a trail of activity for further evaluations including, information sensitive data being altered or moved to another location by workers.

Impact

With this solution, the bank was able to enhance their threat intelligence and threat mitigation capabilities while meeting regulatory compliance on an ongoing basis.

Enhancing access controls to improve site safety

Representative data sources

- Workers' biometric data

Representative technology areas

- Activity sensors and connected devices (facial recognition and automated attendance report generation)

Shared value creation

Individual level

- Seamless site access/exit to enhance work effectiveness

Enterprise level

- Streamlined access control
- Improved workplace safety through bolt-ons to existing infrastructure
- Realistic project planning and staffing

Use case maturity

Exploratory	Emerging	**Maturing**

Key challenge[3]

A construction company was looking for a way to verify access of workers (including subcontractors and staff) in their client site. However, the company has limited control over the client's infrastructure including door access, cameras, and entryways.

This was the case in one of their solar project sites in Western Australia where nearly 250 contractors would visit the site daily. The company required all workers accessing the site to complete a check-in process.

As the majority of its staff would enter the site around the same time, it was essential for the check-in process to be fast and efficient to prevent long queues while maintaining the site's safety.

Solution and approach

The company installed a 40-foot sea container with three bidirectional gates for entry and exit that used facial recognition to authenticate the worker's movement.

The worker movement on the site was fast yet secure. The system provided clear visibility about all workers on the site and their entry and exit times for automated attendance reports. Accurate attendance data enabled project managers to gauge real progress on a project (for example, days remaining to completion, workers required, and more) and data across projects could be leveraged for future planning and staffing projections.

Comprehensive data from the site also helped project managers assess situations in case of any accidents or mishaps.

Impact

The solution allowed the organization to improve their business operations by streamlining their site access for the subcontractors and their staff. The modular container access setup allowed the company to install this solution on any customer site.

Leveraging location-based insights to improve compliance

Representative data sources

- Workers' location data

Representative technology areas

- Location intelligence (VPN and location from where work apps are accessed)

Shared value creation

Individual level

- Automatic sharing of location data without the need for active inputs

Enterprise level

- Compliance with tax regulations

Use case maturity

Exploratory	Emerging	**Maturing**

Key challenge[4]

A social media company offered a remote work policy to all its workers. However, the company observed that workers would often play a geographical paycheck arbitrage–continuing to draw the same compensation while moving to a more affordable location with a lower cost of living.

Early in 2022, the company asked their workers to update their base locations to adjust their salaries according to the local cost of living. In addition to driving a fair compensation structure, the company also wanted to ensure full adherence to local tax laws based on the actual location of their workers.

Solution and approach

The company informed its workers that their location data will be accessed via the company VPN and IP address of devices used to access the company's apps. This passive source of location data provided accurate and real-time information about workers' locations to ensure regulatory compliance.

Impact

This approach enabled the company to adjust compensation structures based on workers' locations. Additionally, this effort can enable the company to improve their compliance to tax laws based on actual location of workers.

Providing the right tools to the workforce to safeguard data

Representative data sources

- Data from collaboration apps

Representative technology areas

- AI (text analytics)

Shared value creation

Individual level

- Better understanding of compliance processes
- Improved satisfaction at work

Enterprise level

- Threat identification and mitigation
- Regulatory compliance

Society level

- Increased data security of customers' data

Use case maturity

Exploratory	Emerging	**Maturing**

Key challenge[5]

A telecommunications company was concerned about data protection risks associated with the use of instant messaging and collaboration platforms within the organization. The company also wanted to enable functionality to search, analyze, and retain the data to respond to legal or regulatory requests.

Solution and approach

With the help of a third-party vendor, the company discovered that their call center workers stored large volumes of personal identifiable information and payment card industry data on these platforms which could potentially expose the company to a data breach.

An internal investigation revealed that the workers used these platforms as they had no secure alternative solution to keep track of customer information, thereby increasing compliance risks. The company provided a more secure alternative space for workers to store customer information.

The company also implemented an automated compliance adherence feature to scan for sensitive data in messages exchanged on instant messaging platforms used within the organization. This allowed them to alert and coach their workers on compliance and best practices in real-time.

Impact

The company provided more secure tools to the workers, offering data security while allowing them to work more efficiently in their day-to-day work. This approach increased worker satisfaction as they felt heard and seen by business leadership.

With this solution, the company was able to identify and remediate over 20,000 instances where data pertaining to credit cards were shared.

Endnotes

1 Quantified organization global survey, Deloitte, November 2023.

2 **Fortune 500 Financial Institution Builds Insider Fraud Solution to Protect Customer Data and Meet Regulatory Compliance**, Teramind.

3 **Revolutionising Site Access Control with Innovative Solutions**, Monford Group Pty Ltd, 2023.

4 Robert Freedman, **Should CFOs let remote employees play 'paycheck arbitrage?'**, CFO Dive, December 8 2020.

5 **Helping a Telecom Provider Investigate and Safeguard Confidential Data**, Aware.

Deloitte.