CASE STUDY

Specialty Automotive Insurance Company Transforms Their Enterprise Risk Management Program

OVERVIEW

A large, specialty automotive insurance company is growing and diversifying their historical core business through mergers and acquisitions, bringing new risk to the organization. In the past, security was viewed as overhead and risk was not quantified or tied to the business. Their head of Information Security valued IT risk management but had identified some organizational challenges.

The insurance industry collects, creates and maintains numerous sensitive data points on its customers. This data, however, must be appropriately secured and protected – and with little IT oversight and a non-operational Enterprise Risk Management (ERM) process, senior leadership had no visibility into data-related risks or overall security posture of the company. Additionally, the organization has customers throughout the United States and Canada, and therefore is subjected to numerous state and provincial data privacy regulations as well as the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). They must also achieve and maintain compliance with additional industry security requirements from the Payment Card Industry (PCI).

HOW OPTIV HELPED

Optiv leveraged our Risk Transformation Service (RTS) to address the gap in ERM while assisting an acceleration of the client’s security maturity by building a custom-tailored, ISO-based, IT security risk management program. The program linked risk back to business drivers and enabled justification of security spending while communicating executive-level measurement and risk management. This risk management program covered the full risk lifecycle including identification of risk sources, process for risk analysis, risk prioritization mapping, process for calculating risk treatment options and metrics reporting. Optiv’s Risk consultants tailored supplemental tools and workpapers to aid the client’s rapid adoption. Risk training and tabletop exercises conducted with the client accelerated education and adoption.

SOLUTION

Risk Transformation Service
- Performed a focused Security Strategy Assessment
- Developed tailored operational processes for risk management and assessments
- Established dedicated cyber risk management team
- Conducted a risk tabletop exercise to accelerate client education and adoption

RESULTS
- Raised awareness of cyber risks through executive-level risk measurement and communication
- Enterprise Risk Council (ERC) tabletop exercise identified focus points for ERM Program
- Created and documented risk assessments and repeatable processes
- Provided cyber risk management metrics and reporting
- Transitioned risk management to client operational staff

NEXT STEPS
- Conduct initial Cyber Risk Assessment
- Monitor and report on cyber risk
- Formal Governance, Risk, and Compliance solution
- Third-party risk management program