

## CASE STUDY

# Fraudulent Transaction Illuminates Third-Party Risk

## 32%

of organizations reported lack of internal time/resources to evaluate or monitor third-party risk<sup>1</sup>

### Industry:

Finance

### Trigger Event:

Fraudulent transaction by third-party

### Client Challenges:

- Time and resource constraints
- Limited third-party risk visibility
- Informal security policies for third-party risk management
- Questionnaire and measurement criteria relevance to business risk profile
- Limited expertise in conducting third-party risk assessment and progress measurement

In the summer of 2018, eSentire was engaged by a financial services firm to conduct third-party risk assessments because the firm had experienced a failed audit due to the discovery of a fraudulent transaction from a compromised third party. Being in the heavily regulated financial services industry, the client had a dedicated internal compliance team and a depth understanding of the various risks associated with information security. In an attempt to mature and formalize its security program, a full-time CISO and dedicated security personnel were recruited but program formalization was ultimately unsuccessful due to the scarcity of qualified and available candidates. As a result, responsibility for information security policies and implementation of controls fell back on the cross-functional teamwork of the firm's internal compliance and IT teams.

Collaboration between the cross-functional teams resulted in an improved security posture, but limitations remained in their ability to measure and mitigate third-party risk. Inventory measurement concluded

that over 50 vendors and third parties had network and data access to some degree resulting in potential risk to overall business operations. Unfortunately for the client, risk became consequence during a routine audit, when a transaction with a trusted third party was discovered to be fraudulent, facilitated by a compromised user within their third party network. Investigation revealed the user was compromised from a spear-phishing campaign culminating in substantial financial losses and lengthy time and resource consuming claims processes with their cybersecurity insurance provider.

Realizing the potential implications for repeat and that they may already be compromised by another vendor, the client contracted eSentire's Virtual CISO services, specifically Third-Party Risk Assessments. The firm was assigned a dedicated Virtual CISO Security Strategist with experience working in the financial services industry.

The eSentire Security Strategist immediately went to work helping the client update their third-party risk

<sup>1</sup>eSentire/Spiceworks Third-Party Risk Research, January 2019

policies, formalizing mandatory annual and bi-annual risk assessments of critical vendors based on type and risk profile. eSentire then executed tailored risk assessments on 10 clients that were both critical to continued business operations as well as high-risk profiles. The data from the assessments was compared against eSentire's Security Framework based on NIST foundations, financial industry standards, and specific risk indicators.

The Security Strategist discussed the findings with the client's cross-functional and Executive team and began to develop a pragmatic plan to systematically reduce

risk among the 10 vendors that were subject to the assessment. Satisfied with the progression of the firm's security posture under their Virtual CISO, recruiting efforts were ceased. With the tedious work of creating and conducting the 10 assessments handled by eSentire, IT and compliance teams were able to focus on other projects. Both of these benefits from eSentire's Vendor Risk Assessments resulted in operational cost savings for their business.

**Reach out to learn more.**

**Get Started**

If you're experiencing a security incident or breach contact us  1-866-579-2200

**eSENTIRE**

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit [www.esentire.com](http://www.esentire.com) and follow @eSentire.