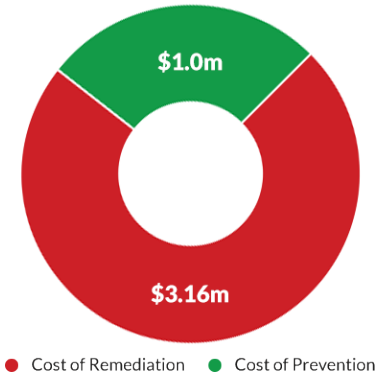
Case Study: Financial Services Fraud Detection

THE CHALLENGE

Financial services institutions use various tools and techniques to prevent fraudulent activity and to quickly mitigate the impact of fraud when it does occur. Research and experience suggest, however, that financial fraud detection could be *significantly* improved.

Annual Costs of Financial Breaches
(in $M for a super-regional bank)



As things stand, breaches have increased by 141 percent since 2011.[1,2] Moreover, 50 percent of fraudulent events are first detected by customers – not by their banks' fraud teams.[3]

During a recent fraud detection project with a major international bank, Haystax Technology gained insight into key factors contributing to the relatively low prevention rate:

- **Detection tools were unable to infer from diverse data sources whether certain activity was likely to be fraudulent.** In isolation many indicators (like type of user) are benign, but collectively they may reveal a fraudulent event taking place. For instance, a new user combined with unusual login activity might well be cause for concern.
- **Detection tools could only search for *known* indicators of fraud.** Anomalous events that *weren't* included in the list of known fraud indicators were either assessed individually or ignored altogether. This approach requires significant manpower, and is often not feasible due to limited resources.
- **A fraud domain model was not used to ensure data was mapped to the appropriate indicator categories.** Without such an organizing structure, data from a single fraudulent event was often thought to be from several different events. Redundancies like this can be a significant drain on resources.

THE SOLUTION

By interviewing subject matter experts across the bank, Haystax constructed a domain model of the bank's specific fraud indicators. The model determines the likelihood that certain evidence (user behavior, user type, user actions) are indicators of fraud, just like a bank's top analyst would do. These indicators on their own may have weak, strong, positive or negative correlations to fraudulent activity, but taken together, these correlations may change. For example, multiple log-ins in a day may not be a strong indicator on its own. However, when paired with an unusual HTML tag ID and an abnormal login device increase the probability that the event has been compromised.

Now operational, the model is a component of the Haystax Constellation Analytics Platform™. The model is run in the platform and ingests data and prioritizes according to likelihood of fraudulent activity. Evidence with the highest probability is tackled first—improving the resource utilization and effectiveness of fraud teams. The solution also identifies anomalous activity that cannot readily be applied to a known fraudulent indicator. This behavior can be separately investigated—and if it turns out to be fraudulent—it can be added to the model.

When Haystax deployed this solution at the international bank, it was able not only to detect the same fraud/malware events the bank was currently detecting but also discovered fraud indicators not previously detected.

Based on these discoveries, we believe financial institutions can save a lot of time and money by developing and deploying a solution that includes these three core elements:

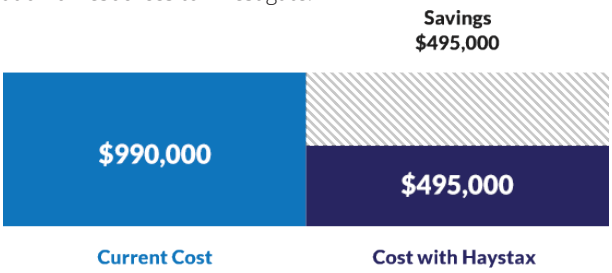
- **A holistic fraud model** that eliminates the need for multiple tools focusing on separate issue areas, and reduces the number of missed attacks.
- **Open and transparent cause-and-effect nodes** that allow model users to drill down into results to discern root causes, and avoid focusing on redundant events.
- **Prioritization and ranking capabilities** that help users respond to the highest-priority events first.

THE ROI

Haystax Technology's solution can result in an average **savings of $1.44M a year**; a return of **five times** the required investment.[a,b]

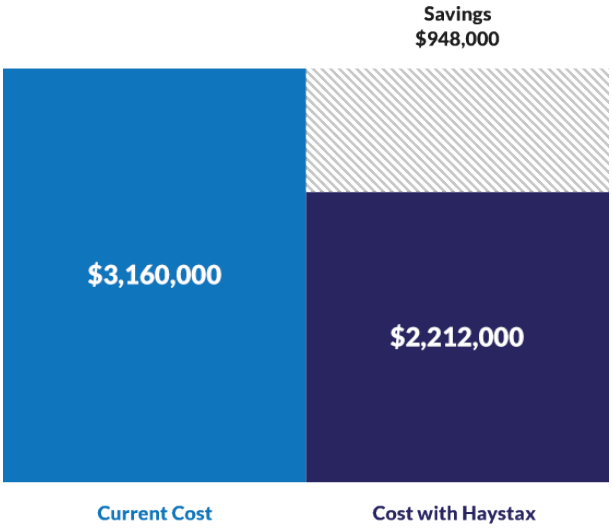
Prevention

Root-Cause Identification: Drill down into the data to determine why it was marked 'interesting,' thereby focusing on root causes and improving allocation of resources to investigate.



Remediation

Prioritize Events: Look at the most 'interesting' events first and thereby decrease time to respond to an attack.



IMPLEMENTING THE SOLUTION

INTEGRATE CONSTELLATION

The model resides in the Constellation Analytics Platform™ and can be integrated into an organization's Security Information and Event Management (SIEM) tools (e.g., Splunk) or related devices. The Constellation Analytics Platform™ allows for real-time processing of structured or unstructured data.

MAP DATA TO MODEL

Once integrated, the data is mapped to Haystax Technology's Fraud Detection Model using Haystax Technology's patented Fusion process of extracting and applying data to the custom model.

PRIORITIZE EVENTS

The model assesses the total data set and evaluates each event to determine the amount of evidence indicating that the event may be compromised. It then assigns the event a probability of compromise. The greater the likelihood the event is compromised, the higher the priority for investigation.

ANALYSTS INVESTIGATE

A fraud risk score is generated and organized from high to low priority. The output is displayed in a dashboard, accessible to authorized personnel. Analysts are able to investigate based on qualitative reasoning and to drill down into the score to determine where the source of risk exists.

REFINE MODEL

The information and knowledge gained from the investigation is used to further refine the model. This allows the model to remain current with existing threats and expand its capabilities to detect other similar attacks.

NOTES

[a] Cost of Remediation: Each record that is breached will cost the bank on average $230 to remediate.[5] Knowing that there are 13,754 malicious/criminal breaches a year,[5] a bank will pay, on average, over $3.16M a year to remediate the breaches. This sum includes the cost of forensic experts, outsourcing hotline support, free credit monitoring, discounts for future products, in-house investigations, in-house communications and losses resulting from customer turnover or diminished customer acquisition rates—not to mention reputation losses and diminished goodwill. By itself, loss of customers and related activity costs a bank $770,000 a year.[5]

[b] Cost of Prevention: Fraud mitigation is currently an exceedingly laborious process, with 75% of transactions flagged as fraudulent by a non-automated process.[4] With heavy emphasis on manual fraud detection, a bank's first line of defense against malicious attacks are analysts. A typical bank may have the following staff in its active fraud prevention department: six to eight junior analysts, two to three senior analysts, and one fraud prevention manager. Salary costs range from between $750,000 to $990,000. At a very basic level, a bank needs a place to store all the data it collects and a way to look at the data. It may choose to have a combination of detection and monitoring tools, but on average will spend between $400,000 and $960,000.

REFERENCES

[1] **Ponemon Institute©.** Cost of Data Breach Study: Global Analysis. 2016.

[2] **Ponemon Institute©.** Cost of Data Breach Study. 2011.

[3] **American Bankers Association©**. ABA Deposit Account Fraud Survey. Washington DC : s.n., 2016.

[4] **LexisNexis® Risk Solutions**. True Cost of Fraud Study. 2015.

[5] **Ponemon Institute©.** Cost of Data Breach Study: Global Analysis. 2015.