Risk Analysis Report
All for $5 Store

By David Umberger

Table of Contents:

Executive summary:

Upon request from company owner, Dan Johnson III, concerning the hacking of card reader machines similar to ATMs, we have conducted a full risk analysis on the point-of-sale card readers for a 50-year-old Washington DC area business called All for $5 Stores LTD. They have 40 stores in a regional area and are 3rd generation family/privately owned and operated.

We first identified the risk analysis components, which included the outputs: assets at risk, threat communities, and the loss event(s).

We also needed to brainstorm and ask questions concerning these inputs: What do we know at this point? What are the assets, threat communities, and loss events? What are the anticipated threat paths? How frequently would the threats occur? How vulnerable is the company to these threats? And What data do we have currently and is it objective for our purposes?

These questions pointed us in the right direction to conduct the risk analysis.

Our approach was to use the risk analysis using the FAIR Basic Risk Assessment Methodology. This was broken down into two stages. Stage 1: Scoping the analysis, which included identifying the asset at risk, threat communities under investigation, and defining the loss event. And stage 2: encompassing evaluate Loss Event Frequency, Estimate Contact Frequency, Estimate Probability of Action, Estimate Threat Event Frequency, Estimate Threat Capability, Estimate Resistance Strength, Vulnerability and Loss Event Frequency.

The assessment results showed the estimated minimum and maximum total loss amounts over a year, which ranged from $60,000 to $19.6 million. This is what the company could experience based on the current risk exposure. This range does not guarantee a loss for every year but what could happen.

The Loss Exceedance Curve visually shows that the more the loss exposure is or how much All for $5 Stores is vulnerable, the greater the possibility of loss is. The company currently has 97.08% vulnerability based on the data given. This curve shows the possibility of the loss exceeding a certain amount (being the loss exposure). For example, 18% probability of a loss >= $8,000,000.

The Primary and Secondary loss breakdown shows us by the number of threat attacks per year, the amount of loss the company could be facing. For example, for Primary loss, if we had 7 threat attacks that year, we could be facing around $66,000 in losses.

Based upon the risk analysis, there were several recommendations made. A few of them are physically check for card skimmers, stress the skimmer training point to employees to look for these devices, upgrade video surveillance equipment, and have a local police presence in the stores near the point-of-sale registers to discourage any activity.

Overview:

We worked with a 50-year-old Washington DC area business called All for $5 Stores LTD on a risk analysis. They have 40 stores in a regional area and are 3rd generation family/privately owned and operated. Their business focuses on food and toiletries to electronics and clothing - a one-stop-shop type of arrangement. The company has maintained a good reputation with its communities and government entities. This is especially important since they have ambitions of opening another 4 stores in the next 24 months and would like to see sales revenues from those soon.

The stores have a similar layout and floor plan with six checkout lanes including point of sale and back-office systems. Payment card usage is 45% debit card, 35% credit card, and 20% EBT cards. This would be consistent in the types of neighborhoods that they are located in since more affluent areas tend to favor more credit card users. The average purchase amount is around $30 so purchases don't tend to be high.

My role as a loss prevention specialist is to analyze physical stores, front and back-office systems, and theft. The company keeps costs down by allowing a contractor to maintain the store equipment but as we will see, this also opens up the door for non-invested intentions. Notably, the video surveillance is not robust with the records only keeping for one month time and reused every 30 days and could miss a device retrieval. However, the company prides itself on being well trained in loss prevention and working with local police on these matters.

Upon request from the company owner, Dan Johnson III, concerning the hacking of store machines similar to ATMs, we have conducted a full risk analysis on the point-of-sale card readers since it appeared after looking at loss prevention, most of the occurrences happened by shoplifting and bad checks. These can be a steady drain of cash flow and consistently hurt the company revenues. Dan is concerned about the negative publicity that data breaches can have and since All for $5 Stores is heavily involved with the local chamber of commerce and community, they want to keep the company reputation strong. We looked specifically at ATM skimmers, which sit on top of the card readers undetected and absorb data for some time, only to be retrieved later and used or sold for exploitation. We pulled together data provided by All for $5 Stores and ran a FAIR risk analysis to provide an estimate of how often and how much the company may be exposed to this form of loss.

Scope:

The first part of knowing the scope will do and not do is to identify the risk analysis components. These would include the outputs: assets at risk, threat communities, and the loss event(s).

Confer about the process of these inputs:

- What do we know at this point?
- What are the assets, threat communities, and loss events?
- What are the anticipated threat paths?
- How frequently would the threats occur?
- How vulnerable is the company to these threats?
- What data do we have currently and is it objective for our purposes?

Conversely, this risk analysis will not handle everything. In identifying the risk analysis components, we may not know anything about them so this information will have to be obtained.

Defining the participants in this analysis is an important part of the process and not all will be primary or secondary stakeholders.

We will not collect endless data where it becomes so much that it becomes endless information. We will find good and relevant data useful for the risk analysis that is more objective.

Lastly, this risk analysis will not stop the risk completely. There will always be the potential for loss since nothing can be guaranteed.

Approach used:

The risk analysis is done using the FAIR Basic Risk Assessment Methodology. This was broken down into two stages:

- Stage 1: Scoping the analysis
    - Identify the asset at risk
    - Identify the threat communities under investigation
    - Define the loss event
- Stage 2: Evaluate Loss Event Frequency (LEF)
    - Estimate Contact Frequency (CF)
    - Estimate Probability of Action (PoA)
    - Estimate Threat Event Frequency (TEF)
    - Estimate Threat Capability (TCap)
    - Estimate Resistance Strength (RS)
    - From the above measures, we can find Vulnerability (Vuln) and Loss Event Frequency (LEF)

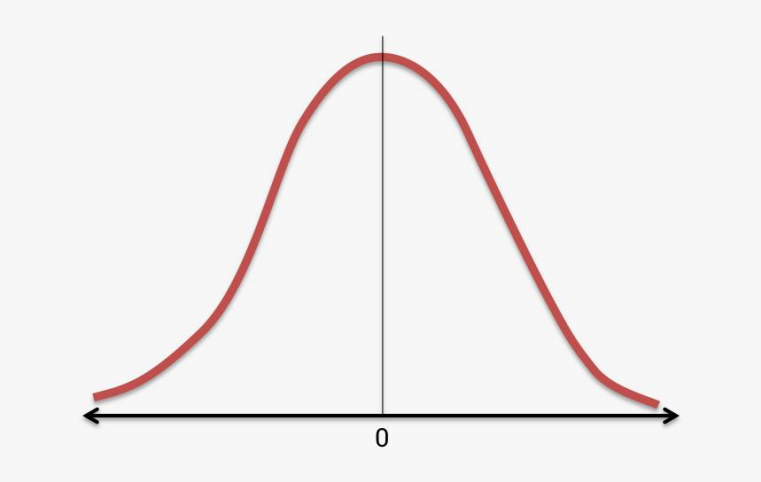
Regarding scoping the risk analysis, we will want to find out:

- Exactly what is the asset?
- What is the community or potential performer?
- How is a loss realized in this analysis?

Regarding the Loss Event Frequency, we want to know:

- How vulnerable the asset is to attack and loss?
- What may affect this vulnerability?
- Where may consequences come from in a loss event that doesn't relate to the asset or the owner? Could they be customers, communities, government, or stakeholders?

Once these questions are reasonably addressed and estimates are obtained for minimum, maximum, and most likely, the FAIR analysis tool will calculate and synthesize this data in several statistical processes which will result from normal bell-shaped distribution curves as shown below.



Risk analysis components:

To help better understand the assessment portions of this report, we describe some of them here. These are referred to throughout the report so it will be helpful to how they apply to our techniques.

Threat Community (TC) is used in the FAIR software explanation as threat sources or threat offenders.

Contact Frequency (CF) looks at how often a dishonest vendor or employee may repeat this threat in a year.

Probability of Action (PoA) considers how serious this dishonest vendor or employee might be to commit the offending action with the presence of store personnel, customers, and video surveillance.

Threat Capability (TCap) considers how possible is it for the dishonest vendor or employee to successfully turn their actions against the asset for a loss. This will give us an idea of how successful this threat could be.

Resistance Strength (RS) measures how serious this dishonest vendor or employee might be by the percentage of how possible this threat may happen, given the presence of other store personnel or video surveillance.

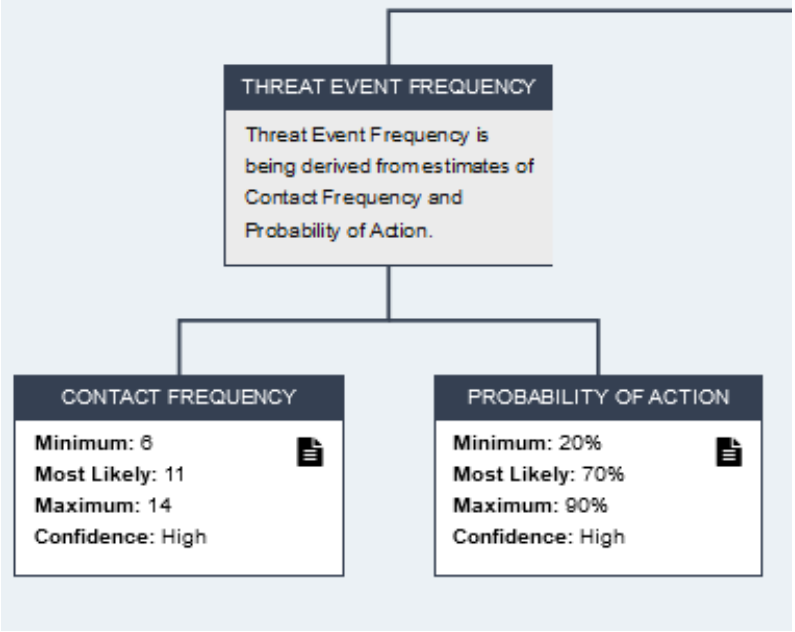
Vulnerability (Vln) is comprised of Threat Capability and Resistance Strength so this measures how susceptible you are with the current safeguards that are in place.

Loss Magnitude (LM) measures the outcome of the risk evaluation comprised of the primary loss which is the estimated asset losses and secondary loss which depends on the successful sale of data and exploitation of that data.

Assessment results:

To obtain our assessment results, we used the software tool FAIR analysis where we obtain the following outcomes. This is a useful tool that calculates an overall risk analysis. To view the FAIR tree in its entirety, see Appendix 1. To view the Loss Exceedance Curve, see Appendix 2 and to view the Summary of Simulation Results, see exhibit 3. Here we will split the FAIR tree and break down the two sides of the tree and look at the components of each. However, before we look at these numbers, we must consider that these results will only be as good as the data provided in our analysis. We should ask the data suppliers if their data is objective and precise? These answers will give us a better understanding of how confident we can be in these findings since they are estimates. A question one must also answer is if the extra time is worth it to obtain more occurrences? Ultimately, one must understand that this is a calculated projection since there are no guarantees.

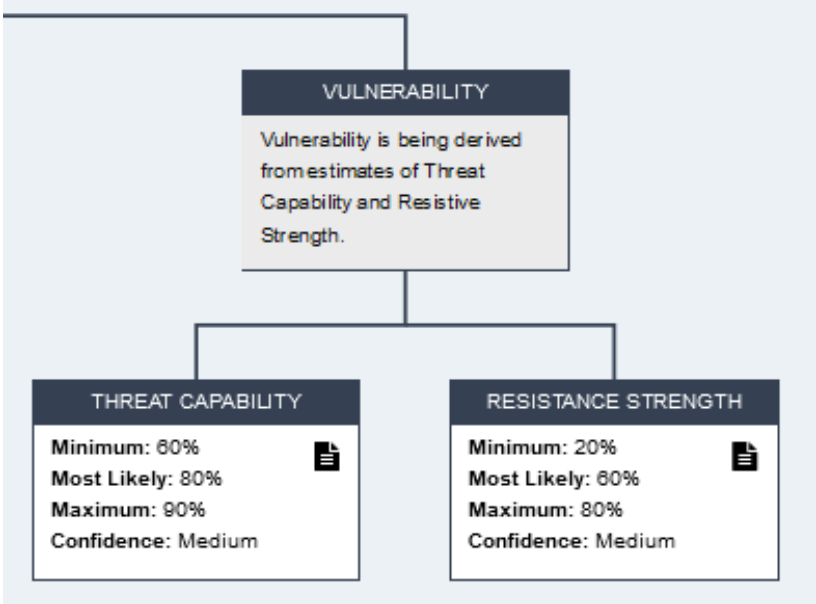
First, we will look at Threat Event Frequency, the left side of the Loss Event Frequency branch, which is derived from the Contact Frequency (CF) and Probability of Action (PoA) components shown below.



In looking at the Contact Frequency, the threat offenders will most likely need about 30 days to capture credit card numbers because they would not want to be pulling the device often, this would presume around 1 time/month per occurrence, thus most likely 11 times/year. Here we will estimate a minimum, maximum, and most likely counts. We are also looking for how confident we are in these estimates. This will give us an idea of how certain this event is likely to occur.

Probability of Action's percentage will measure how possible this threat may happen so we will estimate a minimum, maximum, and most likely percentages. 70% seems fairly reasonable since it is more than 50% likely to occur and would create more of a cautious outlook.

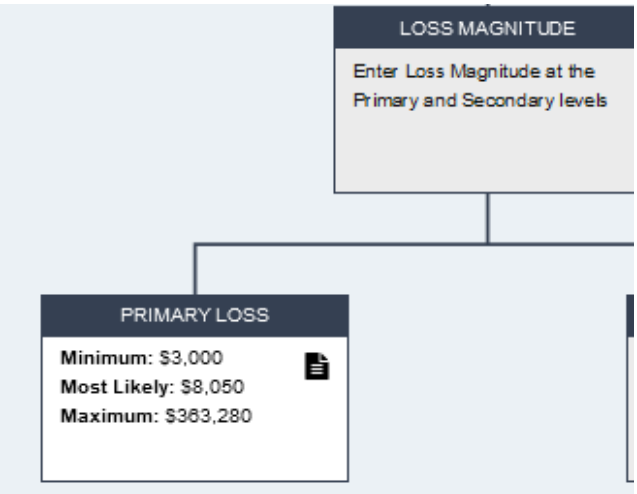
Next, we will look at Vulnerability, the right side of the Loss Event Frequency branch, which is derived from the Threat Capacity (TCap) and Resistance Strength (RS) components shown below.



This Threat Capacity takes the placed skimming device, which remains unknown, and collects data to be retrieved undetected and then sold. The device is then traced back to All for $5 Stores and holding them responsible. Here we will estimate the minimum, maximum, and most likely percentages of this occurring. In this case, the offender would sell the data with a penalty towards All for $5 Stores. We are also looking for how confident we are in these estimates. 80% most likely is fairly high so this is a stronger estimate but with a medium confidence level that this threat is capable of success.

Since Resistance Strength is the percentage of foiling the crime, this component will estimate a minimum, maximum, and most likely percentage of catching the offender. 60% most likely with a medium confidence level seems fairly reasonable since it is more than 50% but not too high and optimistic where it would be unreasonable. One factor to keep in mind-affecting this measure is how much management and staff are is in store and that tapes are reused every 30 days so this could miss a placing or retrieving of a device.

We will now look at the other side of the FAIR Analysis tree. Primary Loss is the left side of the Loss Magnitude branch shown below.

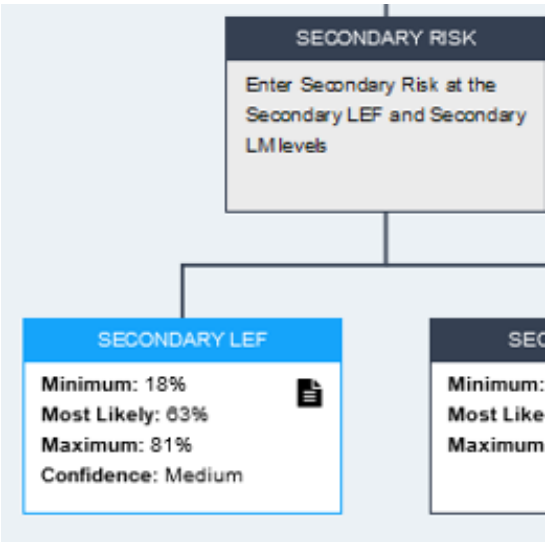


Primary loss is comprised of six factors that directly relate to the loss of assets. Below is the table of data used in the risk analysis. To revisit the subject of data in that the risk analysis is only as good as the data are given. Relating to each factor:

- Productivity – the checkout lane would not be available where a threat attack took place, which would bottleneck the other lanes and could lead to a loss in sales of $2800. This will be more notable during peak season.
- Response – an employee might need to be sent to stores to give a presentation on the exploitation of using these skimming devices. If additional times to review videotapes looking for offenders, this will involve more outflow. Fines and judgments could fall under this factor in the form of attorney fees.
- Replacement – a single card reader costs $668 but will depend on the severity of how many could be skimmed on. $260480 would be a company-wide major problem.
- Fines and judgments – relating to EBT cards, state laws regarding safeguarding credit cards these may not apply and muddled attorney fees can make this uncertain so a $0 is assigned
- Competitive advantage – with a threat attack itself without secondary damage would be no issue
- Reputation – with a threat attack itself without secondary damage would be no issue

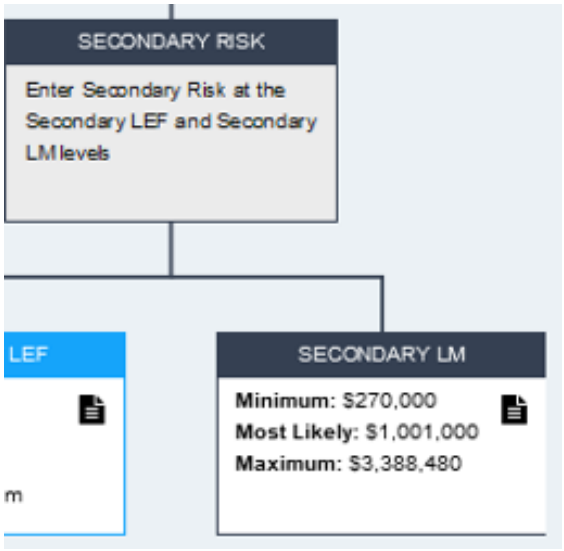
Productivity	Minimum	$0	Most Likely	$50	Maximum	$2,800	Confidence	High
Response	Minimum	$3,000	Most Likely	$6,000	Maximum	$50,000	Confidence	Medium
Replacement	Minimum	$0	Most Likely	$2,000	Maximum	$260,480	Confidence	Medium
Fines & Judgments	Minimum	$0	Most Likely	$0	Maximum	$50,000	Confidence	Medium
Competitive Advantage	Minimum	$0	Most Likely	$0	Maximum	$0	Confidence	Medium
Reputation	Minimum	$0	Most Likely	$0	Maximum	$0	Confidence	Medium

We will now look at Secondary Loss Event Frequency on the left side of the Secondary risk branch shown below.



Secondary loss is the percentage of loss occurrences that already have primary losses and then go on to have secondary losses, therefore primary losses must exist. Consequently, most likely 63% of the primary losses will have a secondary loss resulting from the threat. This number is reasonably high but given this the confidence is medium, this should not be too alarming since the primary losses are not too heavy so exploitation may vary given the offender.

Lastly, we will look at Secondary Loss Magnitude on the right side of the Secondary risk branch shown below.



Secondary loss is comprised of six factors that directly relate to the loss of assets. Below is the table of data used in the risk analysis. To revisit the subject of data in that the risk analysis is only as good as the data are given. Relating to each factor:

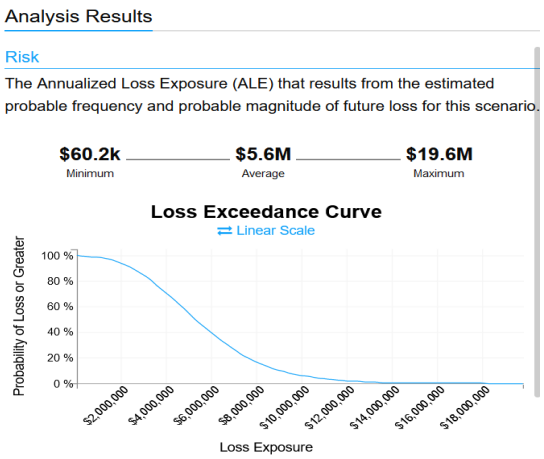
- Productivity – costs for the customer and public communications, as well as gather executive attention or backfill the vacant position. These costs could get higher than anticipated so the most likely $35000 is reasonable.
- Response – organizational costs of hiring a public relations person to communicate and follow-up on the current situation. This cost of hiring someone for this role would be reasonable around $24000
- Replacement – anything above the primary loss is not acceptable to the public. $260480 would be a company-wide major problem.
- Fines and judgments – these will be unfortunate as a result of the attack situation and with 4200 plaintiffs and possibly 4000 fraudulent claims, this could potentially add up to around $420000
- Competitive advantage – considering 30 years of business built on positive word of mouth marketing, a negative situation would reverse this effect and help their competitors leading to lost business
- Reputation – since this is a privately owned company, a threat attack would negatively impact any further store expansion and further sales revenue from new stores. This attack would also heavily affect the company's short-term revenues given that there could be political pressure to change business practices until the problems are resolved.

Productivity	Minimum	$12,000	Most Likely	$35,000	Maximum	$60,000	Confidence	Medium
Response	Minimum	$8,000	Most Likely	$24,000	Maximum	$48,000	Confidence	Medium
Replacement	Minimum	$0	Most Likely	$0	Maximum	$260,480	Confidence	High
Fines & Judgments	Minimum	$0	Most Likely	$42,000	Maximum	$420,000	Confidence	Medium
Competitive Advantage	Minimum	$250,000	Most Likely	$500,000	Maximum	$1,000,000	Confidence	Medium
Reputation	Minimum	$0	Most Likely	$400,000	Maximum	$1,600,000	Confidence	Medium

The Annualized Loss Exposure shows the estimated minimum and maximum total loss amounts over a year that All for $5 Stores could experience based on the current risk exposure. An important point to note here is that this range does not guarantee a loss for every year but what could happen.

The Loss Exceedance Curve visually shows that the more the loss exposure is or how much All for $5 Stores is vulnerable, the greater the possibility of loss is. As we can see as told by the numbers below, at 97.08% vulnerability. This shows the possibility of the loss exceeding a certain amount (being the loss exposure). This could also be called the exceedance probability curve where we apply the statistical simulations by calculations along with the range of results and finding the percent of values that are greater than or equal to segments of the range.

Along the x-axis is the annualized loss exposure for the given risk scenario considered in the analysis. Along the y-axis is the possibility of a loss being greater than the intersection with the x-axis, from 0 to 100%. For example, a 40% probability of a loss >= $6,000,000 and a 70% probability of a loss >= $4,000,000



Summary of Simulation Results

This section below shows a Primary and Secondary loss breakdown of estimated loss frequency and per-event magnitude. This shows us by the number of threat attacks per year, the amount of loss we could be facing. For example, for Primary loss, if we had 2 threat attacks that year, we could be facing around $5900 in losses. Again, this is not to say that a loss will occur but that it could occur. This can allow us to compare analyses to see what level we are comfortable with.

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	2	7.03	11
Loss Magnitude	$5.9k	$66.1k	$241.6k

Secondary

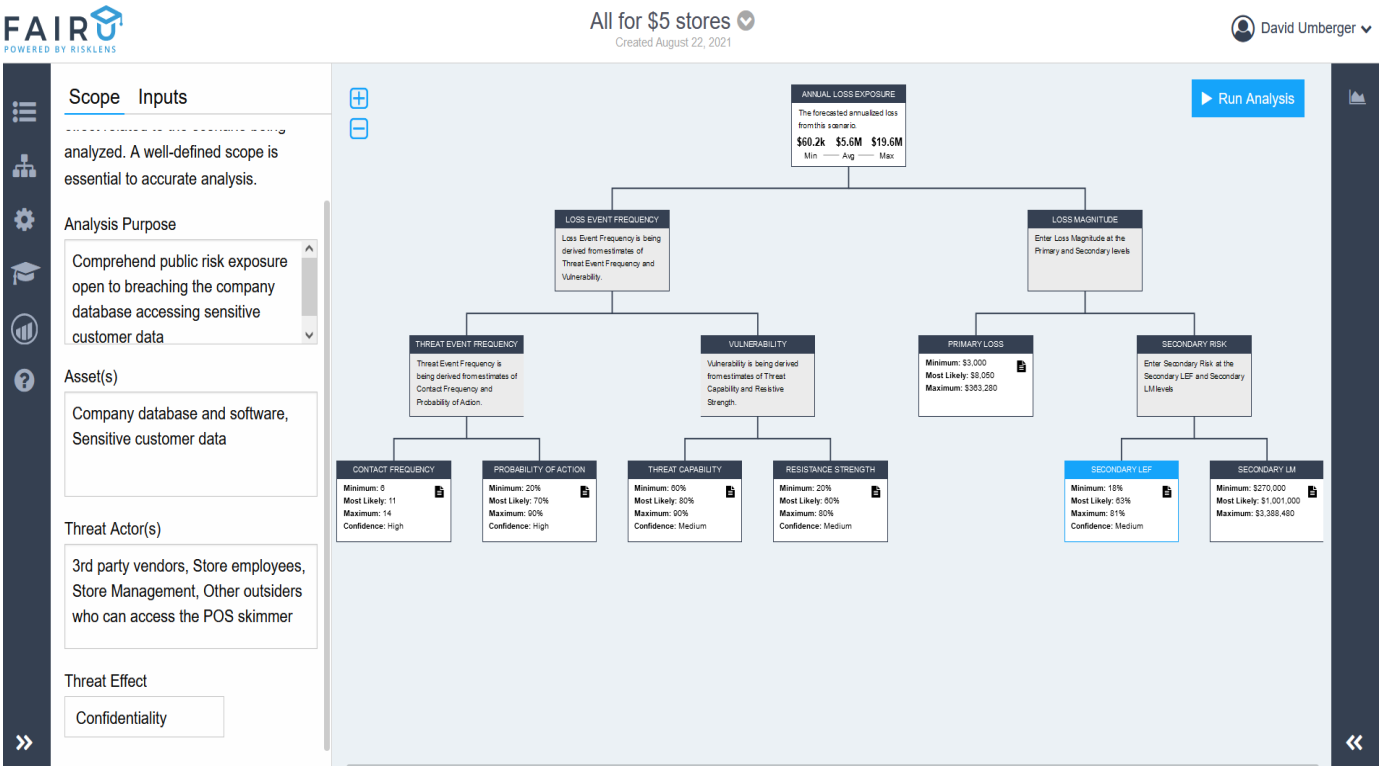
	Min	Avg	Max
Loss Events / Year	0	4.1	10
Loss Magnitude	$416.6k	$1.3M	$2.4M

Vulnerability 97.08%

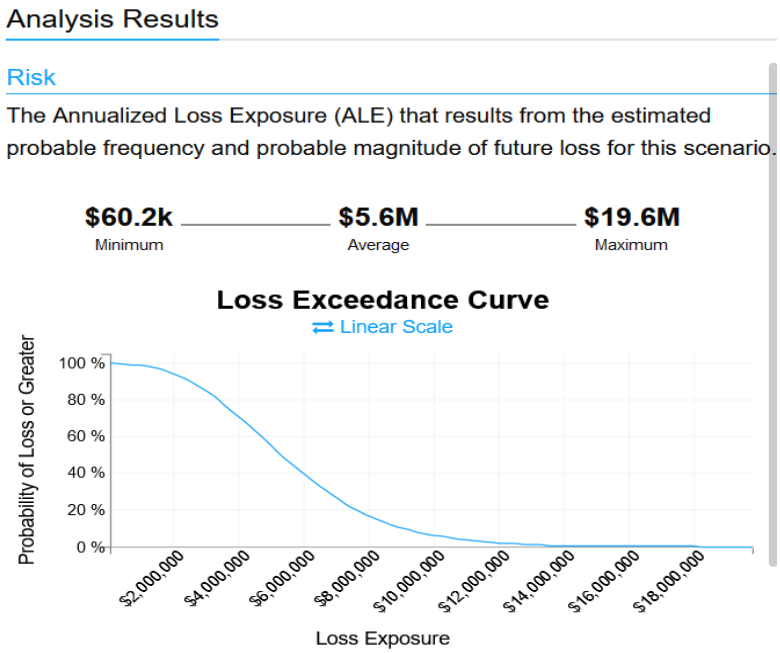
Mitigation recommendations:

Observation:	Recommendation:
There does not appear to be any active checking for card skimmers.	Physically check for card skimmers – this may be the best way to discourage dishonest employees or vendors to use them by actually checking for them on top of the card readers. Given that they need to sit for some time to collect data, there is more of a likelihood that they would sit versus not sit there.
There is nothing mentioned about card skimmer training.	Stress the training point to employees to look for these skimmers and perhaps even offer incentives on apprehending one of them. It would be wise to have additional loss prevention training relating to what to look for in finding them.
There is no mention of upgrading the video surveillance.	Upgrade the video surveillance equipment since the card skimmer can self-power for 45 days, this is longer than the period of videotapes.
Even though there is a good relationship with local police, there is no mention of involving them regarding these.	Have local police presence in the stores near the point-of-sale registers to discourage any activity. Even one officer would be sufficient.
Nothing is mentioned about networking with other companies regarding this issue.	Get the word out about these skimmers more to other local businesses. The more information is available is helpful to everyone.
The company did not mention anything about heavily going after the offenders.	Stiffer penalties for offenders – prosecute to the full extent of the law.
There is no mention of how they are handling this with the public.	Publicly project that they are on the lookout and addressing the issue. This would let their customer base that they are taking this seriously and ensure that no one is taken by surprise. This would also help reputation.
It appears there is an intermittent presence.	More consistent management and staff near the point-of-sale registers to discourage activity.
Contractors are allowed to work unsupervised.	Contractors are monitored when on-site.
Card readers appear to be generic market versions.	Investigate card readers that would reject skimmers physically or the software would not work with one.

Appendices:



Appendix 1 - FAIR Analysis Tree



Appendix 2 – Loss Exceedance Curve

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	2	7.03	11
Loss Magnitude	$5.9k	$66.1k	$241.6k

Secondary

	Min	Avg	Max
Loss Events / Year	0	4.1	10
Loss Magnitude	$416.6k	$1.3M	$2.4M

Vulnerability

97.08%

Appendix 3 – Summary of Simulation Results