Risk Analysis of Rane Logistics (ISC2)

Risk Analysis Objectives

1) Review business impacts of risks, issues, and related terms
2) Discover data collection mechanisms and approaches to organizing risk data
3) Explore effective methods and techniques for risk and issue elicitation
4) Conduct qualitative and quantitative risk and issue analysis
5) Investigate what and how to communicate risks and issues with stakeholders

Rane Logistics Overview

Welcome to Rane Logistics

Rane Logistics is a for-profit company specializing in over-the-road (OTR) truck-based intermodal shipping and the arrangement of temporary warehousing at inland ports. In addition to provisioning intermodal container shipping with our fleet of company-owned semi tractors, we provide several types of trailers, including lowboys, refrigerated trailers, flatbeds, dry vans (enclosed and Conestoga), and bulk load hoppers, as well as different tanker capabilities, such as corrosive chemicals, flammables, and food products.

Size and Location

Rane Logistics is located in the United States, with one headquarters facility that conducts all business and the coordination of warehouse and transport operations and schedules. Serving customers primarily in North America, Rane Logistics is also equipped to provide inland and coastal port-to-port trans-shipping services for international clients. Employment numbers include 77 full-time headquarters employees, approximately 1,800 teamsters, and typically anywhere from about 100 to 300 consumer-to-consumer consultants throughout the United States, Mexico, and Canada.

Business Culture

The culture here at Rane Logistics is entrepreneurial, with a close eye on the competition and a willingness to expand whenever possible. In business for over 50 years, we have bought out two competitors to obtain their clients and routes. We have a high appetite for risk, and our company-owned fleet says a lot about the care we have for our teamsters. We are one of the few companies that doesn't pay by the mile—we pay per hour, including traffic delays, and loading and unloading time. In this manner we ensure a predictable—and relatively high—paycheck each week, even if no miles are driven.

Mission Essential Functions (MEFs)

The mission essential functions (MEFs) at Rane Logistics include several domains that drive the company and culture forward. Each of these domains is managed by a chief or director with a number of assistants, as necessary. Simply put, the work, or functions, that

occur here on a day-to-day basis fall into two broad categories, those that are essential to accomplishing our mission, and those that aren't. This doesn't mean that a non-essential function isn't important; it means that the business can survive without it, albeit perhaps not as well. To put this in context, I should spend a moment talking about the difference between a "mission" and a "vision," as they are often confused. An organization's vision is something they will not accomplish; it simply sets the stage upon which they will perform.

Missions are small, achievable goals that both align to and work towards the vision.

Here are our identified MEFs

- The "Teamster Operations Center," or TOC, a 24/7/365 communications and control facility that tracks the location of all vehicles and warehoused cargo every minute of every day.
- Financial operations, including budgets, payroll, expenses, insurance, and other accounts receivable and payable. Not contracts, which are handled by the legal department (see below).
- Business development activities, including marketing and sales, as well as looking for competitors that might be ripe for purchase.
- Asset lifecycle management activities, including acquisition, oversight of transport vehicle maintenance, and final disposition of all company-owned transport (primarily tractors, trailers, and specialty vehicles).
- Training academy, providing initial on-boarding training, safety training, jurisdiction-specific legal training, specialty training (such as hazardous cargo or over-size loads), and mandatory annual refresher training.
- Communication and computing technology operations, cybersecurity, and maintenance.
- Human resources, including recruiting.
- On-staff legal and security personnel, to handle contracts, lawsuits, accident investigation, theft, and operator complaints.

As CEO, I understand that technology needs to be at the forefront of our operations. Innovation and research into new technologies is encouraged, and I stress that above all, technology should promote safety and ensure that we can stay in touch with the teamsters and track the cargo, at all times, no matter where they are.

Parts Management and Maintenance

Vehicles and parts are procured from only two manufacturers to simplify parts management and maintenance. Lubrication, oils, and fuels (L-O-Fs) are obtained locally when on the road, although accounts are held with three major Truckstop companies to simplify expense charges and billing. Lodging and meal vendors also have preferred providers, but the teamsters can stop anywhere and use a corporate credit card or cash, and expense report the charge. We contract with independent owner-operators when necessary and use a single broker to simplify the paperwork. Satellite, Internet, and cellular technology are in use, along with a single cloud service provider to schedule and communicate with deployed teamsters.

Leading Change

At Rane Logistics, we try to stay ahead of the curve by adopting IoT devices, high-quality satellite communications, and cloud services. As a long-standing family-owned and -operated business, we were one of the first companies to host a public facing “load board” and allow customers to request services through our website. Our company vision is to increase safety while improving the management of the fleet and the cargo we are responsible for. Currently, we are exploring driver-assisted and driverless technologies, in order to better understand them. We recognize that change is inevitable, but want to lead it, not be led by it.

Part 1: Discovering Risk

Meet Kyle

Hi, I'm Kyle McKenna, chief information officer (CIO) and also serving in the role of chief information security officer (CISO) at Rane Logistics. I was a teamster in my younger days but found a second career in IT, and over a span of 30 years, I have spent time in almost every aspect of this business, becoming the CIO eight years ago. I am given a large amount of autonomy in my role, and a large budget to go with it, giving me the ability to research cutting-edge technologies. Safety is the top priority, and I have just discovered an issue that puts the safety of our teamsters at risk.

IoT Systems

One of the IoT systems, a tire sensor installed on every wheel, was just found to have a bug. These devices report on the condition of the tire with real-time telemetry. They were found to not be reporting the true condition of the tire, thus increasing the likelihood of a tire failure on the road. Come to find out the company that produced the sensor has been out of business for a year, so there is no chance of a fix or patch from them. I need to write up a report to the CEO, and I believe the Butterfly Effect of the sensor company closing has led to a black swan, which means we may be in need of better risk analysis. Help me review my notes on these terms before I submit the report.

The Butterfly Effect is a scientific principle that revealed that a very small change in circumstances in one location can lead to a very large and sometimes catastrophic change in another location. The connection or relationship between the two events isn't always immediately apparent. This effect is often described with a hypothetical situation in which a butterfly flapping its wings in one part of the world causes a disturbance in the environment, and that small change ripples and grows exponentially, resulting in a massive disturbance in another part of the world.

document-butterfly_effect.pdf

Black Swan: A term coined by Nicholas Taleb, the term Black Swan is defined by three elements. A Black Swan is a unique, unplanned outlier that has a large (often global) impact. Because these far-reaching impacts were unpredictable, they can only be explained after the fact.

document-black_swan_events.pdf

Overview of Threats, Threat Actors, and Threat Vectors:

document-threats.pdf

Overview of Vulnerabilites

document-vulnerabilities.pdf

Overview of Risks, Issues, and Opportunities

document-risk-issues-opportunities.pdf

Overview of Mitigations, Capitalizations and Remediations

document-mitigations.pdf

Risk Assessment vs Risk Analysis

The distinct elements of risk assessment methodology are a risk assessment process together with a risk model, assessment approach and analysis approach

- COSO: “risk assessment is all about measuring and prioritizing risks so that risk levels are managed within defined tolerance thresholds without being over controlled or foregoing desirable opportunities
- We need to analyze those risks in order to prioritize

<u>So, our goal is to assess risk, in order to analyze it?</u>

Simplest way to assess risk is to say that you think the likelihood of a risk manifesting into an issue or opportunity is either low, medium or moderate, or high,

- Now your definition of those labels can be whatever you want
- You can do same thing with costs you’ll incur from an issue or the money you’ll make from an opportunity => known as “single point or deterministic values” and this is what you get from qualitative risk assessments
    - Works only if you want relative comparisons
    - Ex) risk A is high but compared to risk B it’s only maybe medium risk
    - In some organizations and situations that comparison is good enough

Quantitative Analysis: if you want to understand risks from standpoint of their duration or you want to apply a price tag

- Gives you quantities or numbers (remember they’re estimates so honest assessor will give range of estimates just like meteorologist will give % chance on rain)
    - There is an element of uncertainty, but quantitative report can show you that as well

Process to Analyzing Risk

1) Define Terms and identify what needs to be understood or discovered in process
2) Then work with small groups, teams or individuals to elicit some of the risks and issues present in your organization and you organize what you've elicited into a selected framework
3) Then you can begin process of analyzing your findings and identifying potential mitigations or remediations
4) Finally, you'll want to act on findings, and implement changes that best suit your organization
5) Remember: ongoing process

Broadly speaking you want to gain a multidimensional understanding of risks, issues and opportunities. You want to know how they could affect both the technical and non-technical aspects of the business. You're concerned with protecting the work that your organization does in tandem with the specific processes that make it happen, in other words, you want to protect the value stream. Underlying that is the desire to protect the technology that enables the value stream to keep flowing. However, you can't get caught up in the technology alone. You have to provide a layer of abstraction. Cybersecurity is not a product in and out of itself, it's part of the value stream, but the user need not understand the underlying mechanics of implementing it. Good Cybersecurity places an abstraction layer between the implementation and the user.

The failure of the tire sensors, that was a technical issue that affected at least two-related business processes, the safe transportation of your client's goods, and the timely transportation of those goods. Going forward, when you evaluate risks that come with technologies, you also need to evaluate risks to the business processes that rely on those technologies and you'll classify those as specific risks. Now the non-technical workers won't understand or even care why the technology let them down. They depend on technical workers to handle that, and to alert them when it's going to impact their ability to do their jobs. That's use providing the abstraction layer. Ultimately a specific risk may pertain to more than just part of business, it may have enterprise-wide ramifications, and I'll address that next.

How would you define a specific risk vs a company or enterprise-wide risk?

The failure of the tire sensors did not impact your entire company, it could have, if not for your quick investigation and remediation. From a public relation standpoint, getting in front of the problem and controlling the message, that enables you to appear safety-conscious, proactive, and transparent to your customers. In fact, it is my understanding that early numbers from accounting department indicate a net boost in sales and new customers. So the line between a specific risk and an enterprise risk, is a fuzzy one, with one often morphing into the other, and under other circumstances, risks come to light at the enterprise level and never pertain to a specific process or technology".

Do these risks tie into our company's mission-essential functions?

Simply put, the work or function, that occur here on a day-to-day basis fall into two broad categories: those that are essential to accomplishing your mission and those that are not. That doesn't mean that a non-essential function isn't important, it just means that the business can survive without it, albeit perhaps not as well.

Creating the Risk Team

Chief Operations Officer (COO): allows to connect the dots across the entire organization
Next to CEO and CFO, he is the only one in the company with insight into every aspect of the business

Chief Financial Officer (CFO): has overarching view of the company's financial posture and can see how risks, issues, and opportunities can affect that posture

Chief Information Officer (CIO) & Chief Information Security Officer (CISO): perspective into the technology is needed in this meeting

Director of Human Resources (HR): oversees new hires and understands the diverse needs of staff at Rane Logistics. Position enables to view risks, issues, and opportunities from the standpoint of human capital and resources

Manager of Accounting (Budgets): there is a financial component to all risks, issues, and opportunities. Can provide detailed accounting data as this position manages company's budget

Manager of Emerging Technologies: work in analyzing alternative technologies and developing cost/benefit analysis are also tasks performed when analyzing risk

Manager of Fleet Maintenance & Teamster Deployments: could provide insights regarding risks or issues preventing operational efficiency of the fleet as this position maintains vehicle servicing and inspection records and is well versed on current needs of fleet
Helps plan realistic routes and delivery schedules

Senior Teamster: Less than load (LTL) & Full Truck Load (FTL) Logistics: position's cross-functions work, coupled with the relationships he has built, enables him to look at risks from the customer's viewpoint, as well as inside the company
Works cross-functionally with various people and departments within Rane Logistics, maintaining a good working relationship with teamsters, customers, cand company distribution centers and is very knowledgeable

Senior Teamster: Speciality & Intermodal Logistics: position's ability to consider the impact of diverse elements, such as legislation, industry trends, and driverless trucks indicates that he sees what the future may hold

- Important skill to have when assessing risk

Senior Teamster: Tank & Bulk Load Logistics: responsible for overseeing tank and bulk load logistics

- Experience transporting hazardous material and bulk-load cargo indicates that he's the type to carefully consider potential impacts before committing to a course of action.
- Ideally, every risk team should have at least one member with that mindset

Part 2: Organizing Risk

Risks and Boundaries

The truth to risk is that it takes time and the level of effort is very high when you're starting out

- When you have enough information to prioritize the work, you'll also have some data around which to determine level of effort moving forward

In an organization this size, you'll typically see a risk and compliance team of 4-14 people because there are so many variables that go into determining optimal team size and composition

Setting boundaries: What are we protecting?

- Critical that we always define exactly what it is we're protecting
- Called "security authorization boundary/certification boundary/assessment boundary"
- Only responsible for protecting what's inside boundary not outside

Two Types of Boundaries:

- Physical
- Logical

Boundaries don't just include things, but also processes and concepts

Conventional Method: group assets by what they are or what they do
Ex) IT Department can have group called "servers"

We group assets by their inherent risks, which exist when controls are missing or insufficiently implemented, and residual risk, the uncertainty left over after you've controlled or mitigated the inherent risks to the extend possible

- Now you can set boundaries

You need to tailor your approach because no-one size fits all

Sometime there are risks that are both an opportunity and negative risk
Ex) Increasing highway speed limits provides opportunity for more deliveries, but also brings upon greater risks of accidents and fatalities

People often look at risk in terms of technology, specifically hackers penetrating networks, ransomware etc.

- The security of our technology can't be decoupled from the security of our company
- No one in the company has a job that doesn't depend on technology at some level

The security of the company assets only possible if everyone takes responsibility for protecting them

Old cybersecurity adage: "security is everyone's responsibility"

We want to see everything that folks see as risks, issues, or opportunities
Important to define the company's mission essential functions (MEFs)

- Rane Logistics has a single mission, which we describe as the multimodal transportation of freight. For the business to thrive and accomplish that mission consistently, we have a list of mission essential functions that highlight vehicle an cargo tracking, financial operations, business development, and asset life cycle management activities. As well as training academy

Reviewing Approach Options for Elicited Risks and Issues

1) Attack trees and attack-based approaches

This is the oldest approach to protecting cyber assets. Originally, it was singularly applied. However, over the years it's been found to be most effective when used in combination with one or both of the following systems for scoring the vulnerabilities and weaknesses of data sources.

- The CVSS – Common Vulnerability Scoring System.
- The CWE – Common Weakness Enumeration.

2) Risk and Issue-Based

These approaches are based on broadly held common risks and issues or risk modeling tools such as the following:

- OWASP Top 10 – Open Web Application Security Project Top 10 Security Risks.
- PASTA – Process for Attack Simulation and Threat Analysis.

3) Threat-Based

Threat-based approaches use threat modeling tools, such as the following:

- STRIDE – Spoofing identities, tampering with data, repudiation, information disclosure, denial of service, elevation of privilege.
- DREAD – Damage potential, Reproducibility, Exploitability, Affected users, Discoverability.
- VAST – Visual, Agile, and Simple Threat modeling method
    - This method uses highly scalable automation to produce two types of threat models, operational and application models.
        - Operational models use data flow diagrams (DFDs) to look at how an attacker could leverage information.
        - Application models describe threats to the processes and the way in which these threats flow from one component to another, or from one area of the business to another. This type of modelling is well structured for integration with DevOps workflows.
    - This type of modelling is well-structured for integration with DevOps workflows.

- Quantitative TMM – Quantitative Threat Modeling Method
    - This method builds attack trees based on STRIDE, then looks at the attributes of attacks categorized in the tree to identify dependencies between them. It refers to the CVSS to assign scores to the components of the attacks

4) Human-Centric

These human-centric threat modelling approaches include the following

- Trike – This approach looks at a system's users (actors), their CRUD (Creating, Reading, Updating, Deleting) actions, noting whether a given action is allowed, disallowed, or needs to have rules applied for the action to occur. A rule tree (decision tree) is applied as needed.
    - A data flow diagram (DFD) is applied to identify two types of STRIDE threats, denial-of-service or elevation-of-privilege.
    - Risks and issues are then assessed on a five-point scale from the standpoint of CRUD actions.
    - Actors are evaluated from two viewpoints, a five-point scale for the "presumption of risk," and a three-point scale as to the likelihood of them performing a given action.
- Security Cards - This approach looks at an adversarial triad (an adversary's resources, methods, and motives) and its human impact.
- PnG – This method is particularly useful in Agile environments, as it relates directly to the personas in User Stories and Features, although it can be adapted to any "user."

5) Privacy-Based

LINDDUN – Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, Noncompliance.

6) Hybrid

HTMM – The Hybrid Threat Modeling Method combines the following:
- Two human-based approaches, such as security cards and/or PnG (Persona non Grata).
- A requirements-based approach, such as SQUARE – Security Quality Requirements Engineering Method.

7) Multi-Dimensional

- The Open Group - FAIR – Factor Analysis of Information Risk. This approach looks at assets from a loss perspective and tries to determine the probability (likelihood) that a threat actor will succeed, thus resulting in a loss.
- Carnegie Mellon University's Software Engineering Institute (SEI) - OCTAVE (and OCTAVE Allegro) – Operationally Critical Threat, Asset, and Vulnerability Evaluation. This approach is designed to identify risks and issues that are enterprise-wide, or organizational, in scope. It isn't specific to a given system or technology. As such, it is strategic and holistic in nature. OCTAVE Allegro is a streamlined, asset-centric approach to the original OCTAVE.

8) Control-Centric

- The RMF – Risk Management Framework. This method, a favorite in the U.S. Federal Government, starts by categorizing a given system or technology based on the impact to the agency if said system is compromised. Impact is rated only as low, moderate, or high (effectively a deterministic single point qualitative analysis). Systems are classified as minor, major, or part of a general support system (GSS).

Selecting Approach

We have narrowed-down the approach we will use between FAIR and OCTAVE

- Reason why there are so many approaches is because somebody wasn't satisfied with the available approaches at the time
- The important thing here is to justify the approach that you're going to follow and not be afraid to adjust it if it isn't working for you
- Having the flexibility/agility to adapt your approach is ideal
- Outline intended approach in writing, so everyone is reading from same script
- Document the decisions you made, the reason why you chose them and what you discovered when you used a given approach
- Using a discipline approach to proactively look for risks and analyzing them to the extend possible, that supplies the evidence that you're trying to perform diligence and apply that care

Analyzing Selected Approaches

After looking at OCTAVE Allegro and FAIR in more detail, the team decides to create a unique approach tailored to their specific needs.

OCTAVE Allegro	Rane Logistics	FAIR Steps:	FAIR Stages:
Step 1 Establish risk management criteria	**Step 1** Identify the processes that support the MEFs	**Step 1** Identify the asset at risk	**Stage 1** Identify Scenario Components
Step 2 Develop information asset profile	**Step 2** Identify the technology that supports those processes	**Step 2** Identify the threat community under consideration	**Stage 2** Evaluate Loss Event Frequency (LEF)
Step 3 Identify information asset containers	**Step 3** Elicit multi-dimensional risks*	**Step 3** Establish the probable Threat Event Frequency (TEF)	
Step 4 Identify areas of concern		**Step 4** Estimate the Threat Capability (TCap)	
Step 5 Identify threat scenarios		**Step 5** Estimate Control Strength (CS)	
Step 6 Identify risks		**Step 6** Derive Vulnerability (Vuln)	
Step 7 Analyze risks	**Step 4** Perform qualitative and quantitative analysis, as appropriate	**Step 7** Derive Loss Event Frequency (LEF)	**Stage 3** Evaluate Probable Loss Magnitude (PLM)

OCTAVE Allegro	Rane Logistics	FAIR Steps:	FAIR Stages:
Step 8 Select mitigation approach	**Step 5** Develop mitigations, remediations, and capitalizations, as appropriate	**Step 8** Estimate worst-case loss	
	Step 6 Deliver findings to leadership for review and approval	**Step 9** Estimate probable loss	**Stage 4** Derive and articulate risk
		Step 10 Derive and articulate risk	

***Step 3 of the approach that Rane Logistics is taking is also known as the "holistic" management of risk. Rane's specific holistic approach was developed by Lloyd Diernisse. It involves eliciting risks, issues, and opportunities, while simultaneously identifying vulnerabilities, threats, and threat actors to the extent possible.*

Elicit Multi-Dimensional Risks Concept

Many people look at risks in the context of technology or people, a part fails or a there's a bug in the software. With people we talk about human error or single point of failure if only one person can do an important task. These are dimensions and there are many more beyond these two

- Ex) Money and time are also dimensions of risk because if not enough of either, can amplify or add to other risks or limit our ability to mitigate them
- The number of dimensions is variable and decided by organization

Why we need both qualitative and quantitative analysis:

- Quantitative analysis is important for a financial standpoint because it helps me understand the relative cost involved and I can guide Clare toward the best risk-based decision or RBD from a business standpoint
- Qualitative Analysis compares one risk to another and tells me that risk A is more likely than risk B, but it doesn't tell what it will cost business or whether we should even spend money trying to mitigate them
- Qualitative analysis can be used to decide between two choices from a result, called "single-point or deterministic result"

Need to develop mitigations, remediations, or capitalizations
Every technology comes with its upside and downside

Part 3: Eliciting Risk

Risks originate in many different areas of an organization. To get the most complete understanding of the risks that Rane is facing, it is critical to talk to people in a variety of roles as they can speak to the risks they see within their areas and may present a different viewpoint. These sessions will help to paint a more holistic picture as not all risks are technical in nature.

I have attached a document for you to review before our session this week. This document provides several examples of prompt lists, which are lists of key topics or areas of concern that prompt people to think about the risks within specific areas. Having these categories often helps employees to think critically about specific risks they may not have otherwise considered. These are all formal lists but are not etched in stone and can be tailored to your organization. Please forward to others attending the meeting and please let me know if you have any questions after you have a chance to review them.

Risk Management Identification Methods

document-prompt_lists.pdf

Selecting the Prompt List

When I think about our vision of increased safety while improving the management of our fleet and protecting the cargo, we are responsible for, it seams PESTLE would provide good overall view of the risks and issues in a variety of areas.

“From experience, I know that political discussions can lead to some unproductive conversations at times with stakeholders. There’s little to be gained from those types of conversations. Based on my years working with the company, I would say we could probably leave off the political issues as these do not necessarily represent a large risk”

- Spoken by CISO/CIO

PESTLE will be chosen without the P => ESTLE will be used to elicit questions

- Economic
- Social
- Technical
- Legal and Regulatory
- Environment Risks

Modifying the Prompt List

Economic Concern: Increase in cost of fuel because it directly impacts the costs that Rane pays to get the customer's goods from point A to point B. They either have to absorb that cost, thus eating into their profits, or pass the cost on to the customer, which may result in losing the customer.

Social Concern: Unmoderated comments are posted on Rane Website because to private companies such as Rane Logistics, comments like this could pose a risk to their reputation. Another example of a social issue for Rane Logistics could be that since they contract drivers, the trucks the contractors drive could have bumper stickers or messages that do not directly align with Rane's policies.

Technical Concern: trucks have been misrouted due to a bug in the global positioning system (GPS) software. This software could present a technical risk if drivers are given misinformation and they are unfamiliar with the route.

Legal & Regulatory Concerns: If passed, legislation changes in Canada would impose additional safety requirements for commercial trucking. For an international company like Rane Logistics that serves all of North America, this legal and regulatory change could affect their ability to do business in Canada.

Environmental Concern: Changes to emission standards could expedite the need for new trucks within their fleet, resulting in social, economic, legal & regulatory, technical and environmental concerns. Along with emissions, this category could also include the size and weight of the trucks or weight limits on bridges and roads and infrastructure as this is the "operating environment" that trucks inhabit. The work culture or work environment such as office space or how people are able to dress could also tie into this category. This term may mean different things to different organizations.

A global pandemic requires areas to temporarily close borders resulting in social, economic, legal & regulatory, technical and environmental concern. The impacts of a global pandemic are far reaching and could impact each of these risk areas. For Rane Logistics, this risk would fall under all of these categories.

Elicitation Training Session

When a risk is identified, it is motivated by a person's way of thinking and this can sometimes lead to bias or the identification of areas that aren't truly risks

- Ex) a manager using waterfall methodology may identify changing requirements or scope creep as an issue whereas a manager using the agile methodology expects and readily accepts rapidly changing requirements would not consider this a risk or issue. People fall back to comfort zones and these biases are often justified by conventional wisdom or politics, but they should be easy to spot and proactively exposed once the risks or issues are reviewed by the larger group, so keep that in mind as you elicit risks

<u>How to Elicit?</u>

Three basic strategies that I want this group to feel very comfortable with as you prepare for your elicitation sessions

- Dipstick questions:
  - If you want to know how much oil in car you pull out dipstick and it tells you how much oil, condition of oil, and condition of engine
  - With dipstick question you get wide range of information back and you may get more than you expect
  - Key thing with question is that you don't know what you're going to get when you elicit question
  - So, asking questions that start with why or what
    - Ex) Why do you do it that way?
    - Ex) What would happen if?
  - Questions that ask why are most critical as they help to get to the root cause of the risk or issue

2) Show-me sessions
  - Sometimes people wont be able to explain the issue they're experiencing or cant answer what or why question
  - Important to ask them to demonstrate or show then
  - Having someone from a different department look over the shoulder of someone demonstrating an issue provides a more collective viewpoint of the risk and can expose other risks as well
  - Asking people to take them back to their office so that you can see what they're seeing, or asking them to share their screen on a video call to demonstrate an issue, that might be the best way to elicit the risk

- Linkages
    - While a long list of risks may be produced, you'll find there are linkages between many of the risks or issues
    - Linkages are a way of connecting the dots that aren't readily visible between risks, issues, or opportunities that, on the surface, don't seem to be related, but after asking questions, you find out they are related
    - The output of an elicitation session is often a bit messy with a whiteboard full of disparate, apparently disconnected risks and issues
    - To make sense and organize things for meaningful analysis, linkages need to be mapped out and sometimes those linkages are a bit messy too
    - The linkages are not always obvious, but they're still important b/c they can help you to discover the root cause of a risk
    - You'll find that many people identify similar risks, issues, or opportunities within organization and they don't even realize there's a connection between what they identify and other departments are identifying

Guiding Considerations for Eliciting Risk

To ensure that you'll identify as many risks as possible without unnecessary investments of time and resources, these principles may help you to craft your approach. I hope it gives you some ideas as to what to consider when it comes to making sense of the elicited risks. It's not unusual to find that for every raw list of 100 elicited risks, the linkages will bring that down to 20 or 30. Further refinement from the first pass of qualitative analysis will reduce that number to something like 5 or 10. Those are the ones that you really end up mitigating or, if they are actually issues or opportunities, remediate or capitalize on

document-considerations.pdf

Eliciting a Variety of Stakeholders

Current Workflow Summary:

1) Identifying the processes that support our mission essential functions
2) Identify the technology that supports those processes
3) Eliciting multi-dimensional risks through risk sessions
4) Performing analysis as appropriate
5) Developing mitigations
6) Delivering Findings for Review

Process Identification/(”Functioned Deconstruction”): performed by observing and questioning how people do their jobs and how technologies support those jobs
Ex) financial operations, considered a mission essential function

- To perform said functions, many discreet step-by-step processes are followed by the people throughout the organization, not just in the finance department
- Often these processes aren’t documented, or the documentation hasn’t been updated to reflect how the process has evolved over time
- Direct observation and questioning will elicit an understanding of how people execute these processes today thereby ensuring that the essential function is performed
- To see how the processes are identified, let’s review the work of the truck service that technicians at Rane Logistics and how they interact with financial operations

Organize Elicitation Sessions

Organize Elicitation Sessions in Two Ways:

1) Separate groups into departmental teams, after all, these are teams used to working together, they'll have an in-depth knowledge of any particular issue
2) Organize groups across the layers of management: this inter-departmental meeting allows for stakeholders, such as department heads, from different areas to share

We decided to organized sessions by organizing groups across the layers of management.

- Having people at the same managerial level in room also tends to allow for a more open line of communication
- If a manager is going to say something critical, sometimes they're only going to say it around other managers
- During elicitation, you can almost always find a linkage to some other department or area

Guiding Considerations for Eliciting Risk:

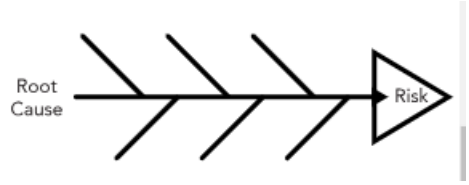
document-considerations (1).pdf

Elicited Risks and Issues:

document-elicited_risks.pdf

Part 4: Analyzing Risk (Quantitatively and Qualitatively)

To uncover the root cause, let's borrow a technique used in tracing the origin of faults, known as a fishbone diagram. Although the use of this tool dates back nearly a century, it was popularized by Kaoru Ishikawa in the 1960s, who worked on developing quality management processes at the Kawasaki Shipyards in Japan. Today it is one of the seven fundamental tools used for quality management, and the fishbone diagram is often called an Ishikawa diagram, in honor of Mr. Ishikawa's work. He is internationally recognized as one of the founding fathers of modern management techniques. Here is one example:



<u>Discovering Root Causes</u>

To understand root cause of a problem, we always ask the question "Why?"

Example:

The branches/Bones of the Ishikawa diagram should be able to explain the place of origin for each risk

- To fill-in diagram we well use a series of why questions to understand why we believe this is a risk, or to figure out where the risk originated

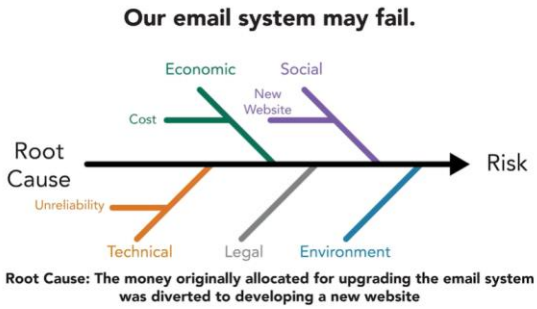
<u>Why do we feel that the email failed?</u>

- The system is old and no money in budget
- System is unreliable

Why isn't money available and why can't we afford to upgrade or replace email system?

- Business decision was made months ago to build a new interactive website that would put us in front of the competition, raise customer awareness, improve our public relations and bring in more business
- Sounded like a great idea at the time, but it meant diverting funds from some other projects like the email upgrade to finance it
- The thinking at the time was that the additional revenue from the new website could be funneled back to the upgraded projects it came from. Unfortunately, the website project ran over its schedule and budget and a simultaneous increase in email traffic strained the email system

Normally we ask the question "why" no more than five times as we drill down to find the root cause for a given risk



- It's important to keep the root cause in mind as we look for the cause or origins of the other risks
    - We may find that other risks stem from the same root cause and those causes are the real item to tackle as opposed to the risks we listed, which are simply apparent risks
- Performing quantitative and qualitative analysis take time and it does cost money, so we want to ensure that we're investing only in the risks that we need to, which we call the "core risks"
- Remember that a decision is a risk as well, because the wrong decision can result in costing more money and a good decision can result in making more money
- Risk is another word for uncertainty
- When a risk begins to manifest, it can spawn other risks
- The decision to divert funds carried with it the inherent risk that you might need that money for its original purpose sooner than you anticipated
- In the field of strategic risk, there's a saying "you only have two risks and they're the dimensions that define what you can and cannot do. The first one is money

and the second one is time. However, since time is money, you only have one risk and that is the constraint that's imposed by money."

Time and money are known by various terms, including grandfather risks, umbrella risks, mother risks, and top-level risks

- We don't analyze top-level risks directly, instead what we do is we use them to define the output of our analysis of other risks
- Ex) we may say a given risk could have a low, medium, or high impact if it manifests, and we may define low as more than $10,000 but less than $100,000 and 80 person hours of lost productivity. Likewise a medium risk has a potential impact that will cost more than $100,000, but less than $500,000 and the hit to productivity may be more than 80 person hours but no greater than 200, and so on
- So we call the descriptors like low, medium, and high qualitative ratings b/c they're relative to each other, of course
    - A low will have less of an impact than a medium risk, but we don't know about how much more it will have
    - The monetary range is pretty broad with the low rating. Let's face it, we're going to consider a loss or gain of $10,000 to be small compared to $100,000. However, any amount in that range is low compared to the loss or gain of half a million dollars and the same can be said about the number of labor hours involved

One of the very first tasks of performing a qualitative analysis is to define what high, medium and low mean to your company

In consultation with the corporate counsel, the insurance carrier and CFO, we worked out a table showing the appetite, tolerance and threshold for risks that could impact business operations negatively or positively. Keep in mind this table only applies to business functional and project risks. Different tables are used for risks that are specific to safety, mergers and acquisitions and special business initiatives

CEO Clare Rane Says "Rane Logistics describes itself as having a high appetite for business risk and that we are willing to push beyond proven technologies in search of new ways to use innovative technology and practices that give us an edge over our competitors, with respect to serving our customers. Any time you embrace new technologies, you are

embracing the inherent risk that comes with things that haven't been around long enough to prove their viability. We have a low appetite for risk when it comes to safety we don't want to take chances with the safety and security of our employees, our customers, or the public at large. Sometimes those two appetites conflict with each other."

- Example of Confliction: We embraced the new relatively unproven tire sensor technology, but its failure led to a potentially unsafe and therefore unacceptable situation

Risk Rating Table:

document-rootcause-terminology.pdf

Sorting Root Cause

After examining and narrowing risks to top three, number one was:

Number 1: Risk of Vendor Lock-In With Cloud Service Providers

- Good candidate for qualitative analysis because we only need a deterministic single point-value of the likelihood and impact

Three sources of information:

1. Current events, includes immediate future
2. History
3. Institutional knowledge

Are we currently locked into one or more cloud service providers?

- Yes
- Okay, so not just risk, it is an issue. It's only a risk if you think it will happen again

Are you planning to procure more cloud services in the near future?

- Yes
- Okay, so still a risk from the standpoint of current events since that includes your immediate future

Some of the cloud products we want are only available from one vendor so the likelihood of risk is high because some of the cloud products we want are only available from one vendor. The company that makes the products only supports it on their own cloud

The line between a risk and an issue in these scenarios gets a little fuzzy because if you're committed to using a product that's only available from one vendor like that, you're essentially already locked-in, so it is no longer a risk, it is an issue. However, if similar products are available from other vendors and they can be hosted on more than one cloud, this may be a risk b/c you have a choice

Risk Evaluation: this risk has a high probability or likelihood of manifesting

Estimate Potential Cost

Labor Hours: the labor hours may be low if we outsource to another cloud-hosted product or high if we decide to custom build an application in-house

Think of all the custom apps you've built over the years and tell me if any of them have exceeded 2,000 labor hours, or a million dollars in cost?

- No, we only have four developers, but they work fast and deliver quality code on time
- We've been an agile SecDevOps shop for a few years now and the most complex app they've built was turned out by two of them in 12 weeks. They make good salaries, but total cost was around $150,000 including overhead

Worst-case scenario, do you think that custom building your own app instead of buying the cloud-hosted one that you're thinking of, could that cost more than twice what the other app cost?

- No

According to table, that puts risk in medium range for monetary costs and probably labor hours as well, but labor hours can get into high risk

That's the thing about qualitative analysis, it is up to you with your understanding of the current state, and history, and institutional knowledge that you possess (and coder's ability) to determine which rating should apply

- Important to remember that your ratings aren't etched in stone

<u>Risk Assessment Matrix (RAM)</u>

Probability (Likelihood)	Range of Monetary Loss or Gain (Impact if it Manifests)	Range of Labor Hours Loss or Gain (Impact if it Manifests)	Comments
		<80	Absorbed into the cost of doing business.
	$10,001 up to $100,000		Risk Tolerance - Cost: Up to $1M Risk Tolerance - Labor Hours: Up to 2,000 Risk Threshold - Cost: $10K - $1M Risk Threshold - Labor Hours: 80 – 2,000
High (Probable)			

Qualitative Risk Analysis

Qualitative Analysis Tasks

1. Agree on Definitions:
    - Define High, Medium, and Low, in terms of the probability that a risk will manifest into an issue or opportunity.
    - Define those same words in terms of money and time, to provide an idea of what the impact will be from the manifestations.
    - Organize these definitions in a risk rating table, to be used as a standard company reference for qualitative analysis going forward
2. Collect historical data about previous risks and manifestations.
3. Collect current data about risks and manifestations that we are aware of now and/or expect in the immediate future.
4. Seek out and document institutional knowledge about risks and issues or opportunities that may not be common knowledge.
5. Create a Risk Assessment Matrix (RAM) to visually organize the information about the risks.

Collect Historical Data About Previous Risks and Manifestations

Corporate Security Department was asked to send copies of reports involving trespassers or acts of vandalism and theft

- Surprising to hear two or three incidents occur a month.
- Over 100 incident reports along with copies of over two dozen arrest reports.

On review, the reports reveal some people ran away when confronted and were not pursued. The people arrested were those typically charged with trespassing—and those who had stolen or damaged something, usually company property, but sometimes crimes involved the personal property of a teamster or other employee. He noted that in the most serious case of vandalism, the company incurred a $14,000 repair cost. Another $7,000 in labor expenditures for that case, for approximately 100 hours of time devoted to internally investigating the crime, working with the police, and later in court during hearings and an eventual trial. Thus, the total came to $21,000; the company did not reach back to their insurance carrier with a claim as it would have possibly raised the rate they pay for that policy.

Looking through the accounting records, it was discovered that these costs were spread out, which is why the chief knew about only the $14,000 repair cost. Charges were booked against several different budget line items in different departments, including the Corporate Counsel and Human Resources, which is why she didn't recall seeing a single charge on the books for the total amount. A note to speak with the CFO was arranged about

developing a different way of tracking these charges going forward, to make the true costs of incidents more readily apparent and easier to report.

Collect Current Data About Risks and Manifestations

Walk around the campus with security chief to fulfil step three of qualitative process, learning about things currently facing the company, and she was very curious, after what she'd learned from the historical data. Security chief brought to light that there was essentially nothing to prevent anyone from getting on campus, or into the buildings, unescorted. He pointed to problems with outdoor lighting fixtures, the placement of windows, areas that were in shadow due to the sun's position at that time of day, multiple building entrances that were unlocked, and many other concerns. The parking lot lights appeared to have old corroded wiring that ran under the parking lot, and there were not the resources to dig it up and replace it.

Headquarters Building

A three-story headquarters building, with a small parking area for visitors in front and a larger lot behind it for employees. This building houses the corporate offices, training academy, hoteling for teamsters and students staying on campus, and the Teamster Operations Center or TOC, a 24/7/365 communications and control facility that tracks the location of all vehicles and warehoused cargo every minute of every day. This building has a small two-truck loading dock near its southern corner.

The Grinder

Southwest of the headquarters' employee parking lot is "the grinder": eight acres of roads with different surfaces and several mock buildings, a shallow skid pond for practicing vehicle skid handling and recovery, and a runaway truck ramp. This is where academy students learn new skills or practice old ones. This facility sets Rane Logistics apart from many of its competitors and ensures that their drivers are the most highly trained and qualified on the road. Typically, twenty test vehicles are in use at the academy, and classes run year-round, in every type of weather.

VMS Facility

Southeast of the headquarters building is the very large Vehicle Maintenance and Storage (VMS) facility, surrounded on three sides by a large paved area approximately 20 acres in size. The building can simultaneously accommodate 36 vehicles (semi tractors, with or without trailers attached) for maintenance and repair services. The building has four loading docks for delivery of repair parts, cleaning materials, and other supplies near its southern corner. Another parking lot, with a fueling station, can hold as many as 200 full-size rigs, including 50 with double, triple, or oversize loads.

Traffic Control Tower

A six-story traffic control tower, similar to what you see at airports, is located in the middle of the southeast edge of the grinder and has a full 360° view of the facility from the top. It is only occupied when students are using the grinder.

Generating Qualitative Results

Risk Table

Probability (Likelihood)	Range of Monetary Loss or Gain (Impact if it Manifests)	Range of Labor Hours Loss or Gain (Impact if it Manifests)	Comments
Negligible (Rare)	<$10,000	<80	Absorbed into the cost of doing business.
Low (Unusual)	$10,001 up to $100,000	81 up to 400	Risk Tolerance - Cost: Up to $1M Risk Tolerance - Labor Hours: Up to 2,000 Risk Threshold - Cost: $10K -$1M Risk Threshold - Labor Hours: 80 –2,000
Medium (Possible)	$100,001 up to $500,000	400 up to 1,000	
High (Probable)	$500,001 up to $1,000,000	1,001 up to 2,000	
Extremely High (Near Certain)	>$1,000,000	>2,000	Unacceptable if risk manifests negatively. (Avoid) Case-by-case if risk manifests positively. (Consider Carefully)

What probability would you assign to the risk of one or more malicious actors gaining physical access to the Rane Logistics Campus?

- High (Probable) (Possible)
- The combination of current information, history, and the security chief's institutional knowledge means that there is a high probability of another incident.

From the research, what range of monetary loss would you assign to this risk in the event of a one-time manifestation?

- $10,001 up to $100,000 (LOW)
- Account manager, Shante had to do a bit of digging to find the true cost of this incident, but both the original figure and the eventual total put it squarely in the Low rating range.

From the research conducted by Shante, what range of labor hours would you assign to this risk in the event of a one-time manifestation?

- Less than 80 (Negligible)

Shanté had to do a bit of digging to find the other direct labor hours (those beyond the repair labor) of this incident, but it is less than 80, thus earning a Negligible rating. Shanté feels this is a sound estimate but would like to reach out to Michael O'Quinn, Rane Logistics Manager of Emerging Technologies for a more detailed analysis.

Cost Per Incident

Year	Number of Incidents	Total Cost*Ê	(Averaged)Ê
2010Ê	3Ê	$24,000Ê	$8,000Ê
2011Ê	7Ê	$119,000Ê	$17,000Ê
2012Ê	4Ê	$44,000Ê	$11,000Ê
2013Ê	3Ê	$33,000Ê	$11,000Ê
2014Ê	4Ê	$52,000Ê	$13,000Ê
2015Ê	5Ê	$75,000Ê	$15,000Ê
2016Ê	7Ê	$133,000Ê	$19,000Ê
2017Ê	3Ê	$21,000Ê	$7,000Ê
2018Ê	9Ê	$234,000Ê	$26,000Ê
2019Ê	11Ê	$231,000Ê	$21,000Ê

<u>Ensuring Understanding of Quantitative Risk</u>

Best Practice: reach out to as many sources of information as you can, until you found answers that make sense and give you something actionable

- Remember we don't assess risks only for sake of understanding them. We assess to understand them so that we can do something about them. So if the information you're turning up doesn't point toward action, keep digging. But, from what I can see, Shante has found a couple of things that require action. That's not to say that the qualitative analysis of this risk is done for all time. Risk of this nature are not likely to ever go away, so you do have to continuously reevaluate them and see if new actions are called for

Quantitative Analysis

Quantitative analysis focuses more on assigning a statistical numerical rating. It's usually used on the highest priority risks

Monte Carlo Simulation: starts with three values that we put into it:

1) Optimistic (Best Case Scenario)
2) Pessimistic (Worst-Case Scenario)
3) Most-Likely Scenario

Example of Monte Carlo Simulation

Let's say there's a risk that I'll get a flat tire on way home tonight.

- Assuming that I have spare tire ready to go, ready to be used, then the best case scenario for me to change the flat and be on my way is about 20 minutes (that's the time it'll take me to do all the steps required to safely change a tire on the side of the road)
    - Optimistic Value: 20 minutes
- However, murphy's law, says whatever can go wrong, will, so perhaps I'll open the trunk and find that my spare tire is flat or it can't be used for some other reason and then I'll have to wait for a tow truck or possible take a taxi to get home
    a. Worst case (Pessimistic) Value: 2hrs
- Also, looking back on my experience with flat tires over the years and considering how difficult it can be when a lug nut won't come free or maybe I encounter a problem with a jack or other typical annoyances, realistically speaking,
    b. Realistic Value: 25 minutes

PERT (Program Evaluation and Review Technique) Formula

(Optimistic Value + 4 (Most-Likely Value) + Pessimistic Value)/6

Tire Scenario: (20min + 4(25min) + 120min)/6 = 40 minutes is the time we should plan on spending for changing car tire

Note: if there's anything to learn about risk, it is that risk represents uncertainty

**Remember that simulations are estimates and still rely on our input so that maxim of garbage in garbage out still applies and range of probable times goes from initial values that we put in earlier of changing the tire in as little as 20 minutes, up to 120 minutes
Benefit of this is seeing that there is only a 3 % chance of task taking two hours and 50% chance of it taking 47 minutes

Conducting Monte Carlo Analysis

Kyle McKenna (CIO/CISO):
Wow, that's a neat looking program. I'm sure there are other inputs we can use as well. Can money be used for a variable as well as time?

Michael O'Quinn (Rane Logistics Manager of Emerging Technologies):
Yes, in fact that's the piece I didn't show you with my tire-changing scenario. The time or duration is only one side of this. We usually want to know the likelihood of what something will cost, as well. We'll use the ranges in Shanté's risk rating table and the information she dug up about the costs incurred from the various incidents and import them into the simulation. We could also break down the data into meaningful groups. There's a difference between someone who is simply trespassing on our property and someone who steals or vandalizes something. I suggest carving out deliberate damage incidents, typically resulting from criminal activities like vandalism and theft, from the others, because trespassing, by itself, doesn't usually incur meaningful extra costs. Do you agree?

Kyle McKenna:
Absolutely. Thanks to Shanté's thorough analysis, it was easy to separate the criminal incidents and see how often they occurred, as well as the range of costs incurred year by year. I am sure you could simply adjust that in the current data table.
How long will 10,000 runs take?

Michael O'Quinn:
It'll be quick; this is hosted on some powerful dedicated hardware, so it'll only take me a couple of minutes to enter the historical data and maybe another 30 seconds or a minute for the simulations to run. Here we go.

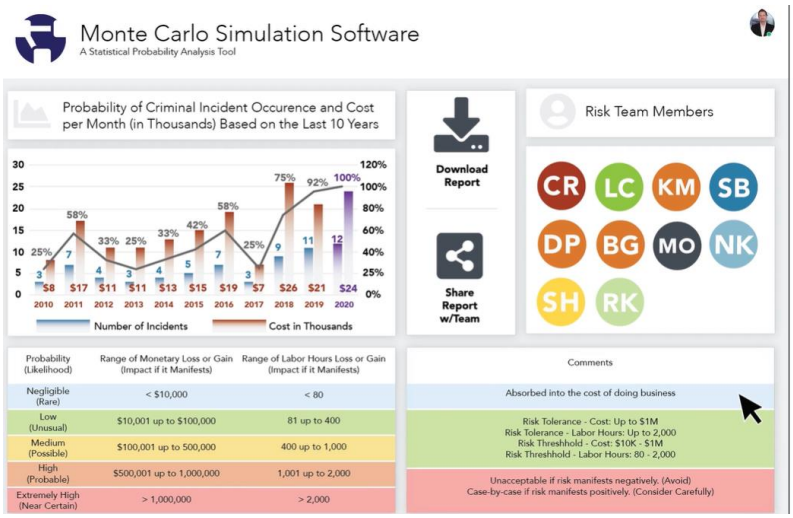
Lower limit cost: $10,000
Lower limit man hours: 80 hrs
Upper limit cost: $1,000,000
Upper limit man hours: 2000hrs

Number of probability runs to perform the input field below: 10,000

Data File Uploaded Into Monte Carlo Software:

Cost Per Incident

Year	Number of Incidents	Total Cost*Ê	(Averaged)Ê
2010Ê	3Ê	$24,000Ê	$8,000Ê
2011Ê	7Ê	$119,000Ê	$17,000Ê
2012Ê	4Ê	$44,000Ê	$11,000Ê
2013Ê	3Ê	$33,000Ê	$11,000Ê
2014Ê	4Ê	$52,000Ê	$13,000Ê
2015Ê	5Ê	$75,000Ê	$15,000Ê
2016Ê	7Ê	$133,000Ê	$19,000Ê
2017Ê	3Ê	$21,000Ê	$7,000Ê
2018Ê	9Ê	$234,000Ê	$26,000Ê
2019Ê	11Ê	$231,000Ê	$21,000Ê



Reviewing Output

Into the simulator we put the number of incidents, costs (Expressed in thousands of dollars), and the years that said incidents occurred

- 10 years of data used to determine trend

<u>Would data that far back be relevant?</u>

Trends are important because the information from any single point in time, and given year, isn't enough to base predictions on. The more historical information you can provide, the more accurate your trend and projections are going to be.

- Ex) We see in 2017, you experienced an unusually low number of incidents, however in 2018 the numbers shot back up again. We also see that the trend indicates an overall increase. The number and cost of incidents per year keeps going up with a couple of exceptions. Back in 2010 we had only three incidents, which is about on every 4 months, which meant that there are 25% chance of a criminal incident occurring in any given month. In 2020, the projection is for 12 incidents or approximately one per month, meaning that likelihood of any incident occurring in one month is 100%. Back in 2010, those incidents cost an average of $8,000 each. 10 years later, we're probably dealing with 12 incidents and average cost will go up to $24,000 per incident.
    c. While the number of incidents increased 4x since 2010, the average cost per incident increased 3x

It is typical, when we're gathering historical information for the software to act on. Over the years, the data that you've collected, and way you collected it, evolved to support changing business needs, this is important to understand when interpreting results. Additionally, each organization is going to have different requirements based off what's important to them and their culture.

There are organizations that just want to look at risk from a financial point-of-view, others are more concerned about time or duration, and others have concerns about resources or skillsets they're going to need to mitigate, or capitalize on the risks that do manifest

- Software currently being used may not be relevant to you later on with the different data

You might get questions along the lines of:

- What if we added this factor?
- What if we looked at the impact of a given mitigation, how would that change the projection?

This is the type of feedback you want, because it means that people are thinking about the data points that you've provided. They're looking for ways to address them

- **These what-if scenarios can only be explored when you perform a qualitative analysis

What-If Scenarios

Michael asked for my help with one of the "what-if" questions he received. Apparently, several people asked about surveillance cameras, at the same time expressing concern about where they'd be placed, whether they're worth the expense, and so on.

Cameras cross a fuzzy line between physical security, cybersecurity, information technology, operational technology, and the Internet of Things, known as IoT, and are a complex topic. People have legitimate privacy concerns, there's something known as the "CSI effect" in which the exaggerated portrayals of crime scene investigation in the media influence public perception, and the good systems are expensive, bringing into question the return on investment, or ROI. These are just a few of the concerns.

Even though the ostensible purpose of cameras is to increase an organization's security posture, they can actually decrease it, if not configured properly. A few years ago, a worm known as the Mirai botnet was used to successfully exploit vulnerable security cameras and other IoT devices, allowing it to propagate throughout networks. It's been used to launch powerful distributed denial-of-service attacks on the Internet. In 2016, it affected a large number of organizations—in both the government and private sectors—in the U.S. and Europe, causing massive outages. Any discussion about procuring devices like cameras needs to also address how we will secure those devices.

On the plus side, there's evidence of the effectiveness of cameras in deterring crimes and, in some cases, providing evidence to solve crimes and obtain convictions. Mike and I conducted some research to obtain numerical data about their effectiveness so we could run a scenario that would give us insight to answer this question: What if we installed outdoor surveillance cameras positioned to cover the parking lots, loading docks, and other publicly accessible areas?

We read a number of studies that have been published by government and government-sponsored entities over the years. We were careful to avoid privately published information from the companies that produce and/or sell camera systems; they have a vested interest in promoting the use of their products.

Every study revealed that cameras can reduce certain types of crime, but by vastly differing amounts. We searched for data from samples that most closely mirrored our intended deployment, but I must caution you that this is not hard data; these are estimates based on input that is not exactly the same as our situation. Please bear that in mind.

Links to Kyle's Research:

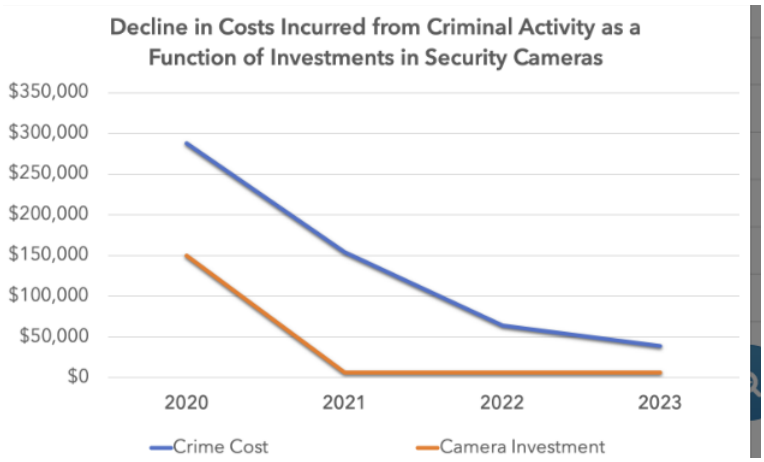
- Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention by the Urban Institute Justice Policy Center.
- Evaluation of Camera Use to Prevent Crime in Commuter Parking Facilities: A Randomized Controlled Trial by the U.S. Department of Justice.
- Video Surveillance of Public Places by The Center for Problem-Oriented Policing and Community Oriented Policing Services at the U.S. Department of Justice.

The Monte Carlo simulations were set up to project three years in advance, based on an assumption that we would install the cameras and have them running by January 1st.

- We placed a three-year limit on it because the technology keeps evolving. If this is successful at cost-effectively reducing criminal incidents at our facility, we'd probably look at replacing these cameras in about three years with new models to benefit from increased capabilities and possibly lower costs. We have a three-year refresh cycle on most of our technology, which is why each of you gets a new laptop and company cell phone every three years.

- We averaged the cost of several models to get a working cost figure. We also factored in the cost of the initial installation and configuration of related equipment, along with an ongoing annual operations and maintenance, or O&M, cost. Up front, our initial investment would be about $150,000. Going forward we could expect to spend about $6,300 per year for O&M.

We ran projections to see how much we could reduce the incidence of vandalism and property theft by spending this money. Every study we read, and all of our other research, revealed it definitely would reduce it; the question for us was whether it was sufficient to justify the investment. Here's what we found:



Despite the steep up-front cost, we could expect an immediate return on our investment.

- That would improve the following year, but after that it starts to flatten out. That's because of the deterrent effect over time. The amount of loss drops and to some extent stabilizes, since less crimes are committed once the word gets out that we have high-quality cameras and we're willing to prosecute with solid evidence.
- We will never completely eliminate criminal activity, but we can substantially reduce it.

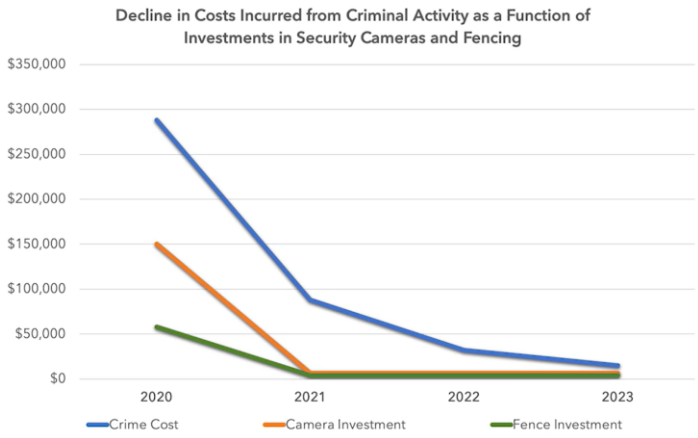
Adjusting Findings

After analysis of security cameras, we ran another what-if scenario, which is to see how the installation of security fencing could mitigate the incidents of vandalism and theft?

First thoughts: implementing security fencing is crime prevention using environmental design

Fencing does have many variables such as type, height, barbed wired, razor wire along top,

- Bottom line: it works and gives a very good return on investment if right type
- Key considerations: having design that you can see through, to avoid blind spots, where criminal activity can be conducted undetected. As well as having sufficient strength to resist cutting, and also has to stand tall enough to make climbing or laddering over the top difficult
- Cost still not as expensive as two doze top of the line security cameras and all of their related equipment
- Annual maintenance costs considerably lower too
- This does make fencing a good alternative to cameras except for fact that we can't see any activity that does take place and doesn't provide strong evidence to prosecute offenders as cameras



Cameras = detective control
Fences = preventative control

Part 5: Communicating Risk

Sharing Findings

**Data is only valuable if it is going to be useful

Final component of risk analysis is to generate reports that are going to communicate risks, remediations and recommendations to the C-suites, board of directors, or any other entity

Include documenting the lessons learned so that this information becomes explicit and enterprise-wide knowledge

Lesson-learned report is general knowledge and does not include the findings regarding the risks within a lesson learned report

- Lesson learned report is general knowledge that can be applied each time risk team meets. That information helps guide organization as they perform a risk assessment, regardless of the type of risk
- Information specific to this round of analysis would be included in a risk analysis report

The risk analysis report is a large report and it's specific to only this set of risks

Risk Analysis Lessons Learned by Rane Logistics:

document-lessons_learned.pdf

Rane Logistic's Top Seven Concerns

document-top_seven_concerns.pdf

Why Only Seven Concerns?

- Elicitation sessions are going to generate a long list of potential risks and issues and that list is usually more than can be tackled in a single round of analysis. If a risk is identified, but not analyzed it just stays on the list, so that the next time the company has time to run the analysis, those already identified risks just move up to the top of the list. They basically sit in the pipeline until the team is ready to analyze them

How often do risk teams commonly meet?

- As with most things, it depends on the organization. In Steve's experience, risk teams commonly meet wither weekly or monthly with the exception of a black swan event, that could increase the need or frequency to meet

Qualitative Analysis Results - Risk 1

Cloud Vendor Lock-in

Probability (Likelihood)	Range of Monetary Loss or Gain (Impact if it Manifests)	Range of Labor Hours Loss or Gain (Impact if it Manifests)	Comments
Negligible		<80	Absorbed into the cost of doing business.
			Risk Tolerance - Cost: Up to $1M Risk Tolerance - Labor Hours: Up to 2,000 Risk Threshold - Cost: $10K - $1M Risk Threshold - Labor Hours: 80 - 2,000
Medium	$100,001 up to $500,000		
High (Probable)			

This is reported as:

Probability: High [-4]
Cost: Medium [-3]
Labor: Negligible [-1]

Total Risk Rating: -8

Using the numbers in the risk rating table, we have a standard way of rating risks, regardless of what they are. It also enables us to compare one risk to another as apples to apples

The labor required is low, but the probability of occurrence is high. There are a few company software developers working on creating some custom software. It is not a priority one item, but we should have the time and budget to work out a mitigation

To Summarize, this type of qualitative analysis generates a risk rating that's a value that represents the combined probability, cost and labor that you could realize if a risk manifests

- Negative risks get negative numbers, positive risks get positive numbers
- Scores can change, so keep that in mind
- Ex) a labor shortage is a negative risk, but if a company is innovative, they might be able to use that to their benefit and bring in interns
    - Intern programs cost very little and they allow the company to offset some of the work. So after six months of looking at the budge, you may find out that you didn't need to hire because by offloading some of the reporting or reporting-related tasks, the programmers were able to write more code and the interns are happy b/c they're getting some real-world experience here, and they're also going to make fantastic candidates to hire by the end of the program
    - So the negative become a positive with appropriate mitigation

Qualitative Analysis Results - Risk 2

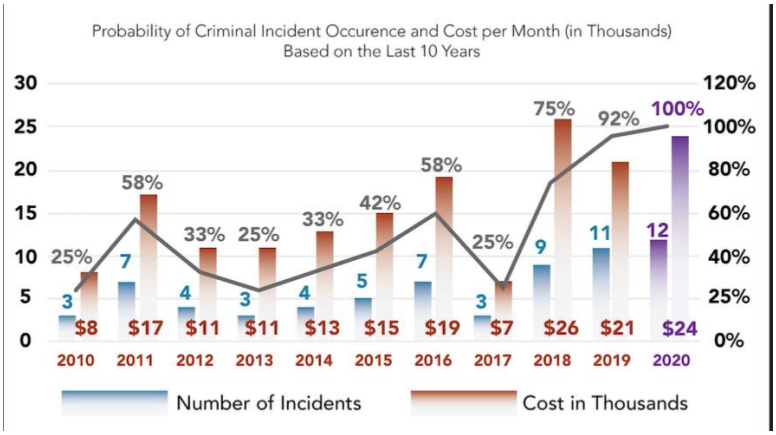
Theft and Damage

Probability (Likelihood)	Range of Monetary Loss or Gain (Impact if it Manifests)	Range of Labor Hours Loss or Gain (Impact if it Manifests)	Comments
Negligible			
Low	$10,001 up to $100,000	81 up to 400	Risk Tolerance - Cost: Up to $1M Risk Tolerance - Labor Hours: Up to 2,000 Risk Threshold - Cost: $10K - $1M Risk Threshold - Labor Hours: 80 – 2,000
Medium			
High (Probable)			

This is reported as:

Probability: High [-4]
Cost: Low [-2]
Labor: Low [-2]

Total Risk Rating: -8



The table was produced by Monte Carlo Simulation

A series of Monte Carlo Risk simulations revealed a projected average of one incident per month with an average cost to us of $20,000. Thus, the approximate annual total cost is expected to be $240,000

Note, without mitigation efforts, the frequency and costs are expected to increase. This means that in any given month, there is 100% chance of an issue happening at a cost of $20,000 per incident

It is clear the trend is going up, so without mitigation there will be an annual cost of at least $240,000

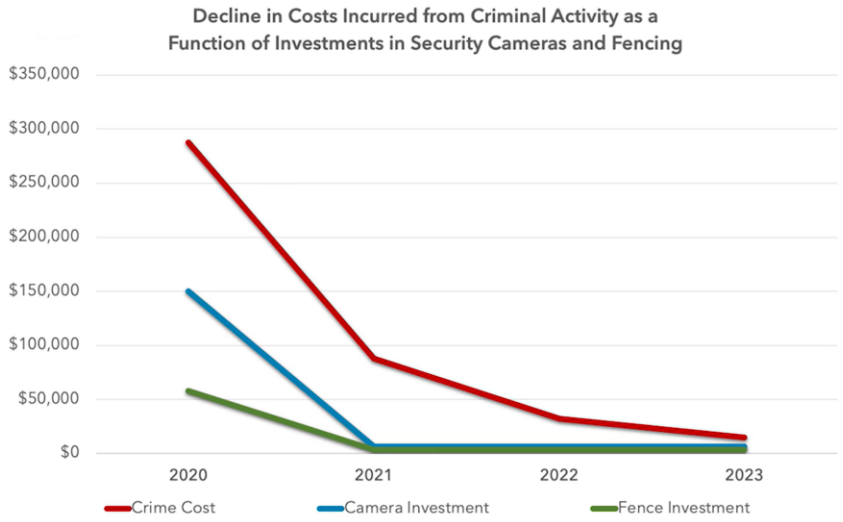
This quantitative analysis supports the qualitative findings

If the general trend is increasing, why did in 2017 we see a reduction in the number of incidents?

- I don't have any specific data to help answer that. There are all types of reasons why crime can go up and down and it doesn't always do so on a consistent basis
- All we can assume is that in 2017, the summers were very hot and winters very cold so that could have affected incidents
- A generally trend found is that crime tends to decrease in bad weather, but of course there are most likely other factors to consider that had an effect
- The trend is always going to be more important to communicate than the outlier
- These trends were done without mitigation, but Monte Carlo software also allows us to consider mitigations

Communicating Mitigation

After looking at the unmitigated cost associated with theft and damage by malicious actors entering the property, the next step was that we took into account the what-if questions posed by the team and ran the Monte Carlo risk simulations on mitigation options



We looked at the use of security cameras and fencing, both individually and combined effect

- We ran three year projections and in each scenario, we saw a quick reduction in both the number of incidents and our costs saving around $200,000 one year out
- Looking at the two what-if scenarios of adding cameras and fencing, the initial investment and ongoing maintenance expenditures are far less than we expected these incidents to cost us if left unmitigated
- Based on this data, the recommended mitigation is to add both fencing and security cameras

Mitigation and remediation are not the same

- Adding fencing and camera will not eliminate the risk of criminal activity, which would be remediation
- Mitigation will lessen the impact

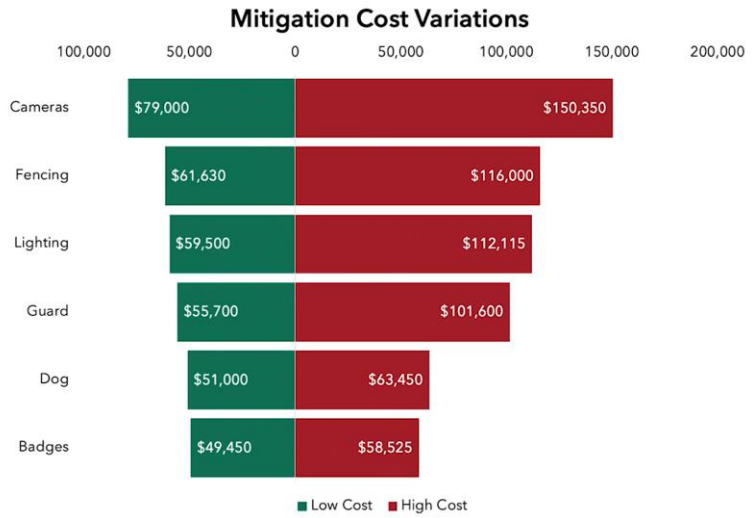
When we mitigate, the cost varies widely

- Ex) Type of camera, fencing, labor to install and so on

To assist the board in understanding the what-if scenario projections that we run in the quantitative analysis, there is another section we will include in the risk analysis report, labeled tornado charts

Tornado charts: depict the variations in costs that come with the various mitigations

- Ex) there is a wide range in terms of quantity, the number of cameras we might purchase, and quality such as the optical resolution or ability of the cameras to work at night



Thus, we could spend around $80,000 or as much as $150,000 depending on the quantity and quality of the cameras we buy

As with the other data, it is important to remember that these are estimated projections
This chart is one of several in your report that illustrates these variables for each of the mitigations we considered
Now, onto the risk ranking of the seven risks we select to analyze this round.

- As you can see, we have ranked the risk in a recommended order of precedence for the board.
- Ranking number provides a way for upper management to see what they should tackle first
- In order to mitigate, we've assigned a value for level of effort. I expect the board will ask for specifics about how much each mitigation is going to cost and this chart helps them clearly visualize these costs
- Note that the last item carriers the most overall risk with a rating of negative 10, however, it's last in priority b/c it won't cost us very much to mitigate this risk
- We recommend the items that have a greater likelihood of impact and involve more money should be higher priorities
- So the fuel price volatility is not something we necessarily need to address right away

Item	Risk Rating	Mitigation (Costs) or Savings	Level of Effort to Implement	Ranking
Malicious Actors	-8	($240,000)	2	3.84
Vendor Lock-in	-8	($150,000)	2	2.40
Firewall Inadequacy	-8	($118,000)	2	1.89
Labor Shortage	-5	($139,000)	2	1.39
Log Reporting	-5	($150,000)	1	0.75
Infrastructure	-3	($79,000)	1	0.24
Fuel Price Volatility	-10	($23,000)	1	0.23

To calculate risk ranking, we take the first three columns, multiply them together, then divide by one million

- We divide by 1 million b/c the mitigation cost is often a large figure, so to get a reasonably succinct number to use in the table, you really do have to divide by a large number. If all of your risks are small in terms of cost, you could divide a smaller number, like a hundred thousand, but in most cases, it's going to be a million

Overview of Risk Assessment Report Elements

document-report_elements.pdf