



[deleted] Scenario Workbook

May 2008

ThoughtQuest LLC
401 Rosemont Avenue
3rd Floor, Rosenstock Hall
Hood College
Frederick, Maryland 21701
(301) 644-3907
www.ThoughtQuest.com

The [deleted] Scenario



December 2007

- An Egyptian student studying bio-chemistry at Cambridge University in the United Kingdom is recruited by al-Qaeda to become a member of the Eurojihad.



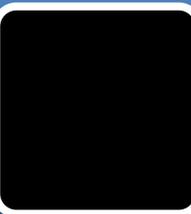
March 2009

- Mushaf Alir Abin's handlers arrange an invitation for him to study at Coleridge University in Des Moines, Iowa.
- Unaware of Abin's terrorist ties he is granted a 30 day student visa by the Immigration and Naturalization Service.
- Before his departure for the United States, Abin is carefully trained on the procedures for culturing staphylococcus aureus and isolating staph enterotoxin.
- Using a hypodermic needle and clear nail polish, he is taught how to introduce staph enterotoxin into plastic Heinz Ketchup containers leaving no visible signs of tampering.



March 15, 2009

- Abin arrives in the United States.
- At Coleridge University under the guise of his research project, Abin cultures staphylococcus aureus and isolates enough staph enterotoxin to poison [deleted].
- He uses materials and equipment readily available at the Coleridge University laboratory.



April 10, 2009

- Abin receives instructions in a secretly coded internet message to take six bottles of poisoned [deleted] and place them on the shelves of six different stores in the Des Moines, Iowa area.
- After completing his task, Abin is instructed to avoid suspicion by completing his research at Coleridge University and then return to Great Britain as scheduled.
- Unbeknownst to Abin, two other al-Qaeda operatives are simultaneously placing contaminated [deleted] on store shelves in San Diego, California and Camden, New Jersey.



April 12, 2009

- The first illnesses are reported at local hospitals. The elderly seem particularly hard hit but no definitive cause can be found.
- Over the next seven days, hundreds of new illnesses are reported in the Des Moines, San Diego and Camden areas.
- While a food borne illness is strongly suspected, staph enterotoxin has not been identified as the source of the poisoning.



April 13, 2009

- Abin leaves the United States and returns to the United Kingdom.



April 17, 2009

- Al-Jazeera announces the release of a new al-Qaeda videotape.
- The tape is authenticated by the Central Intelligence Agency.
- In the tape Ayman al-Zawahri tells the American people that al-Qaeda, in the name of the great Sheik Osama bin-Laden, has just poisoned America's food supply. Al-Zawahri claims that the [deleted] Company is the target of the attack.



April 18, 2009

- The Food and Drug Administration (FDA) confirms that [deleted] containers containing staph enterotoxin have been discovered in the Des Moines, Camden and San Diego areas.
- FDA stops the sales of all [deleted] food products pending the completion of an investigation.
- Heinz stock values plummet.



April 19, 2009

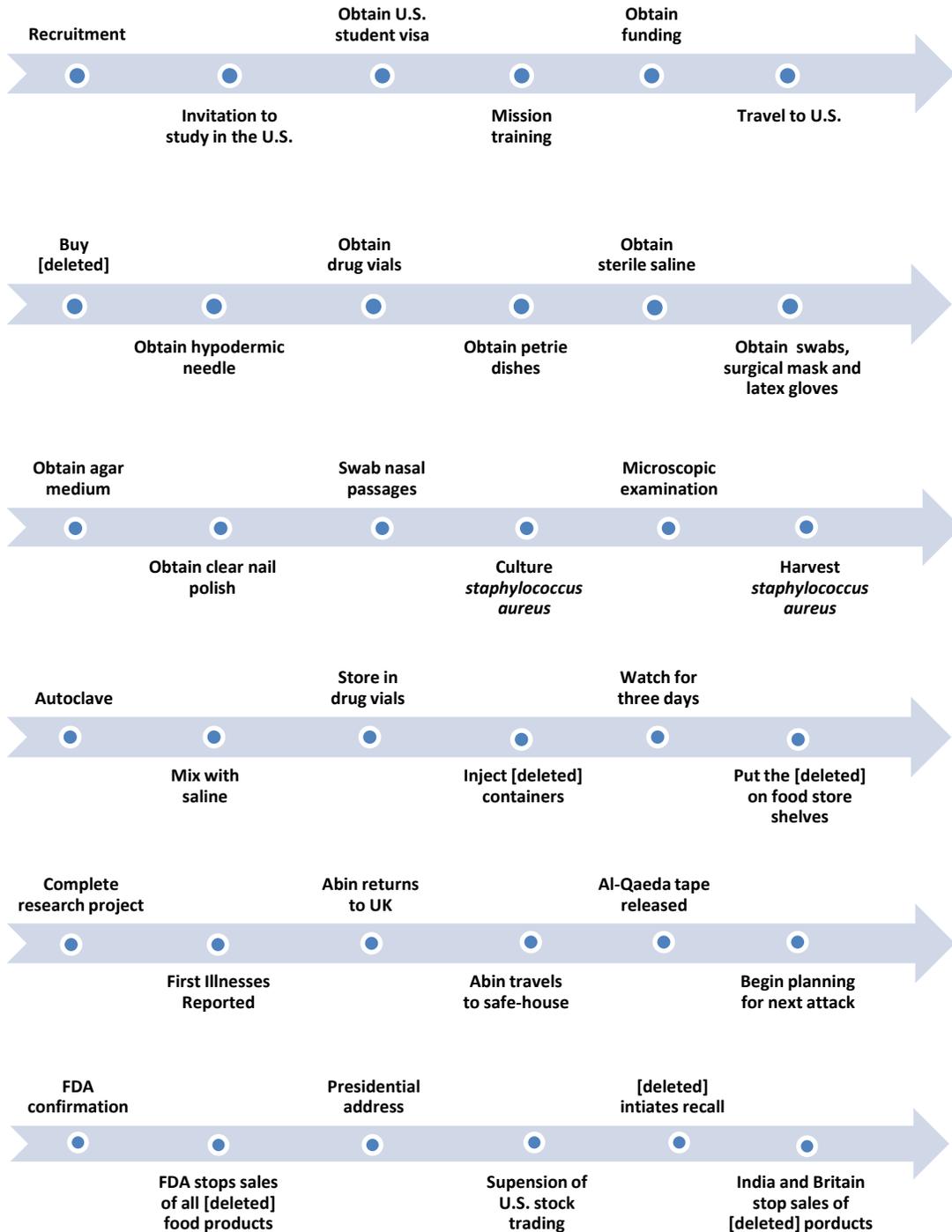
- The President addresses the nation and confirms that the [deleted] Company is the target of an al-Qaeda attack.
- He tells the American people not to panic. He cautions the American public not to eat [deleted] food products until they are told it is safe to do so by the FDA.



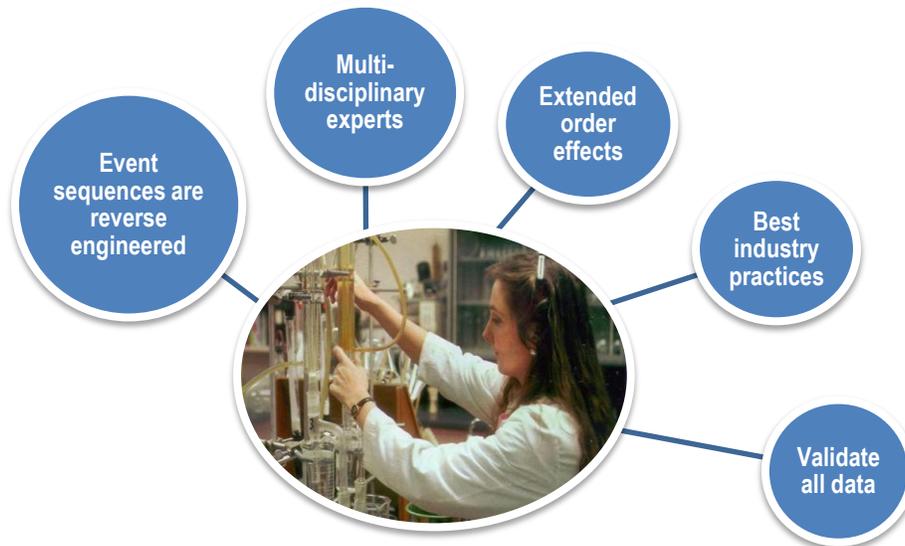
April 20, 2009

- [deleted] temporarily suspends the trading of stock.
- The [deleted] Board of Directors estimates that the poisoning of [deleted] has cost the company nearly \$2.3 billion dollars in lost and anticipated revenues.
- The future remains uncertain.

The [deleted] Event Sequence



Multidisciplinary Teams of Experts



Reverse Engineer Event Sequences



What information, had we known about it before the event occurred, could we have used to...

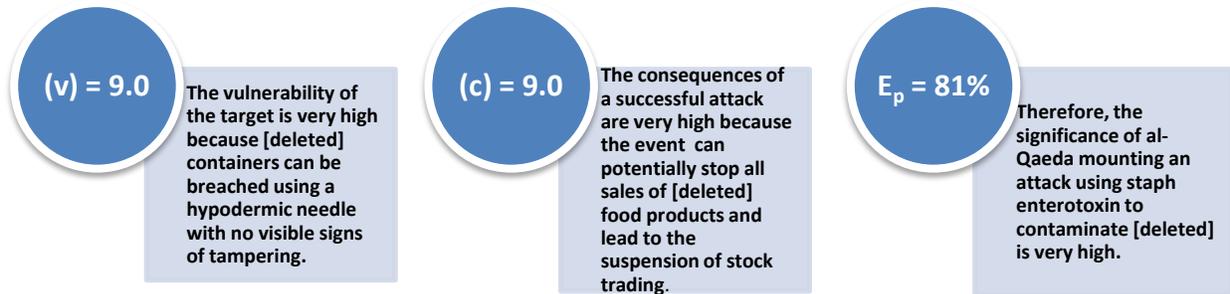
- ✓ Discourage Human actions that create events
- ✓ Discover system abnormalities sooner
- ✓ Diagnose abnormalities quickly and correctly
- ✓ Intervene faster
- ✓ Recover faster
- ✓ Mitigate the long-term consequences of the event

Prioritizing the Event

The CSM Method® states that the priority of an event (E_p) is a function of the level of vulnerability of a critical node (v) multiplied times the value of the worst case consequences that would result from the event (c).

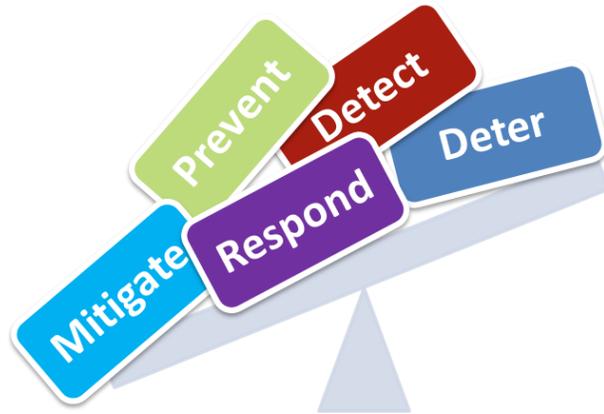
$$E_p = f(v)(c)$$

In the case of the [deleted] scenario this means that the significance of al-Qaeda mounting an attack using staph enterotoxin is very high because:



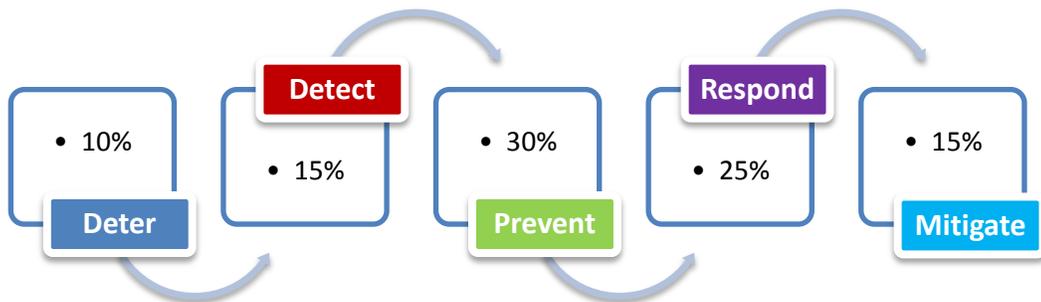
Weighting

Using the CSM Method® risk values can be weighted to reflect the varying importance of preventing events, quickly stopping their escalation, and mitigating the consequences of the event.



Variable Weighting

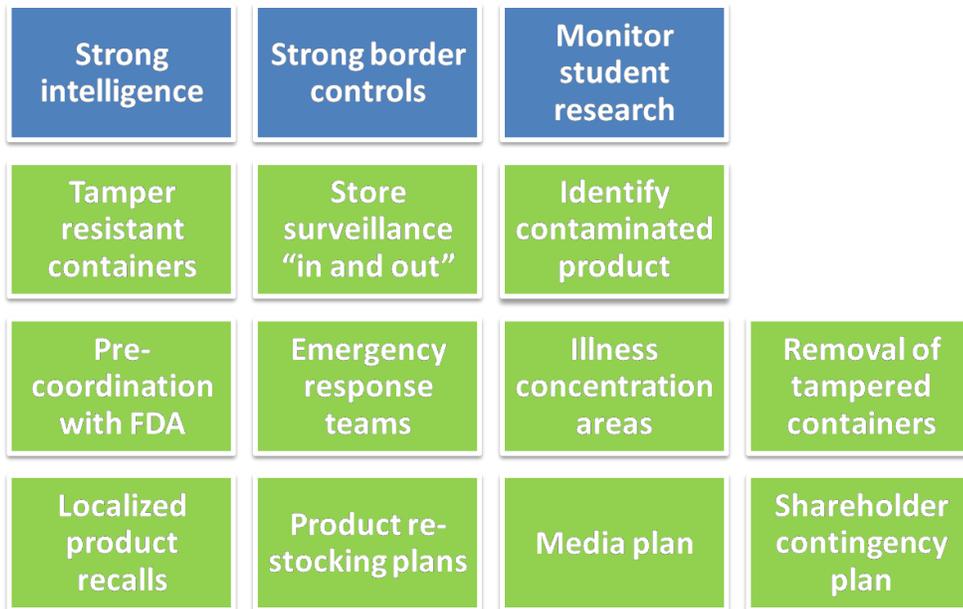
Weighting of risk values for critical nodes can be adjusted.



Weighting adjustments are based on:



Identifying the Critical Nodes



Government

Private Sector

Investments to Deter the Event

What would deter the attack by al-Qaeda?

Critical Node	Deterrence Value	Criteria
Monitor student research	0.65	Scrutiny of Abin’s research project at Coleridge University could have uncovered the al-Qaeda plan.
Strong intelligence	0.60	Strong HUMINT would increase the danger of detection and create an obstacle to effective attack planning.
Strong border controls	0.45	More thorough visa investigation could have detected Abin’s terrorist ties and bogus research agenda.
Tamper resistant containers	0.85	Containers resistant to the use of hypodermic needles that leave visible signs of tampering could have deterred the al-Qaeda attack.
Pre-coordination with FDA	0.80	Al-Qaeda knowledge of effective [deleted] response could cause al-Qaeda to find a softer target.
Store surveillance “in and out”	0.75	Security on the “way in” to food stores increases the possibility of detection.
Identify contaminated product	0.70	The ability of [deleted] emergency response teams to identify staph enterotoxin quickly could cause al-Qaeda to find a softer target.
Removal of tampered containers	0.70	Removal of poisoned [deleted] would limit the spread of illness; al-Qaeda knowledge of effective Heinz response could cause al-Qaeda to find a softer target.
Illness concentration areas	0.65	Early focus on illness concentration areas coupled with quick identification of the attack plan could cause al-Qaeda to find a softer target.
Emergency Response Teams	0.65	Effective emergency response could cause al-Qaeda to find a softer target.
Localized product recalls	0.60	Al-Qaeda knowledge of effective response plans could cause them to find a softer target.
Product re-stocking plans	0.60	Al-Qaeda knowledge of effective [deleted] response could cause them to find a softer target.
Shareholder contingency plan	0.55	The existence of contingency plans that reassure [deleted] investors in the event of attack could cause al-Qaeda to find a softer target.
Media plan	0.50	Effective media plans that stress the efficacy of emergency response can deter attacks.

Investments to Detect the Event

What would detect the al-Qaeda plan before or earlier during the event sequence?

Critical Node	Detection Value	Criteria
Monitor student research	0.85	Scrutiny of Abin's research project at Coleridge University could have uncovered the al-Qaeda plan.
Strong intelligence	0.60	Strong HUMINT would increase the possibility of detection.
Strong border controls	0.45	More thorough visa investigation could have detected Abin's terrorist ties and bogus research agenda.
Tamper resistant containers	0.95	Containers resistant to the use of hypodermic needles that leave visible signs of tampering could reveal al-Qaeda's plans.
Store surveillance "in and out"	0.90	Security on the "way in" to food stores increases the possibility of detection.
Pre-coordination with FDA	0.80	Pre-coordination with FDA to allow deployment of [deleted] emergency response teams is essential to early detection.
Emergency Response Teams	0.75	Effective emergency response could have revealed the source of food poisoning earlier.
Illness concentration areas	0.75	Knowledge of illness concentration areas coupled with emergency response teams could have detected contaminated ketchup sooner.
Identify contaminated product	0.70	The ability of [deleted] emergency response teams to detect staph enterotoxin quickly would identify source of poisoning.
Removal of tampered containers	0.70	The ability of [deleted] emergency response teams to detect staph enterotoxin quickly would allow for removal of contaminated product.
Media plan	0.35	Some detection value based on increased customer awareness.
Localized product recalls	0.30	Some detection value based on increased customer awareness.
Product re-stocking plans	0.10	Little detection value.
Shareholder contingency plan	0.10	Little detection value.

Investments to Prevent the Event

What would interdict the al-Qaeda attack before or during the event sequence?

Critical Node	Prevention Value	Criteria
Monitor student research	0.85	Scrutiny of Abin's research project at Coleridge University could have lead to interdiction.
Strong intelligence	0.60	Strong HUMINT could increase the possibility of detection and interdiction.
Strong border controls	0.45	More thorough visa investigation could have detected Abin's terrorist ties and bogus research agenda and resulted in interdiction.
Tamper resistant containers	0.95	Containers resistant to the use of hypodermic needles that leave visible signs of tampering could reveal al-Qaeda's plans and lead to interdiction.
Store surveillance "in and out"	0.90	Security on the "way in" to food stores increases the possibility of detection and interdiction.
Pre-coordination with FDA	0.80	Pre-coordination with FDA to allow deployment of [deleted] emergency response teams is essential to early detection and interdiction.
Emergency Response Teams	0.75	Effective emergency response could have revealed the source of food poisoning and lead to earlier interdiction of the al-Qaeda attack.
Illness concentration areas	0.75	Knowledge of illness concentration areas coupled with emergency response teams could have detected contaminated [deleted] sooner leading to faster interdiction.
Identify contaminated product	0.70	The ability of [deleted] emergency response teams to detect staph enterotoxin quickly could help to identify source of poisoning and lead to faster interdiction.
Removal of tampered containers	0.70	The ability of [deleted] emergency response teams to detect staph enterotoxin quickly could allow for removal of contaminated product.
Media plan	0.35	Some prevention value based on increased customer awareness.
Localized product recalls	0.30	Some prevention value based on increased customer awareness.
Product re-stocking plans	0.10	Little prevention value.
Shareholder contingency plan	0.10	Little prevention value.

Investments to Respond to the Event

What would improve the response to the event once al-Qaeda initiated their attack?

Critical Node	Response Value	Criteria
Strong intelligence	0.60	Strong HUMINT could increase the possibility of discovering the al-Qaeda attack plan during the event.
Strong border controls	0.10	Little response value.
Monitor student research	0.10	Little response value.
Pre-coordination with FDA	0.95	Pre-coordination with FDA to allow deployment of [deleted] emergency response teams is essential to effective response.
Emergency Response Teams	0.90	Teams of technical personnel capable of identifying the source of contamination are essential to effective response.
Illness concentration areas	0.85	Knowledge of illness concentration areas coupled with emergency response teams are essential to effective response.
Removal of tampered containers	0.75	The ability of [deleted] emergency response teams to detect staph enterotoxin quickly would allow for removal of contaminated product.
Identify contaminated product	0.70	The ability of [deleted] emergency response teams to detect staph enterotoxin quickly could identify the source of poisoning sooner for a more effective response.
Localized product recalls	0.70	Localized product recalls are essential to effective response.
Tamper resistant containers	0.65	Tamper indicating containers would allow on the shelf inspection for contaminated product once the source of the contamination was isolated.
Media plan	0.65	Public awareness can prevent further contamination and panic.
Shareholder contingency plan	0.65	Board responses to an attack can affect stock values.
Product re-stocking plans	0.10	Little response value.
Store surveillance "in and out"	0.10	Little response value.

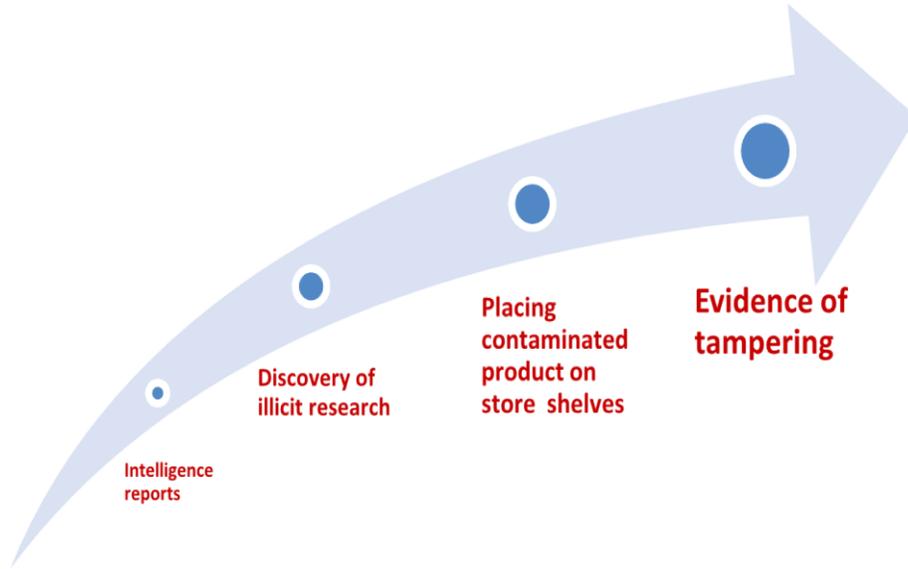
Investments to Mitigate the Event

What would mitigate the consequences of the al-Qaeda attack?

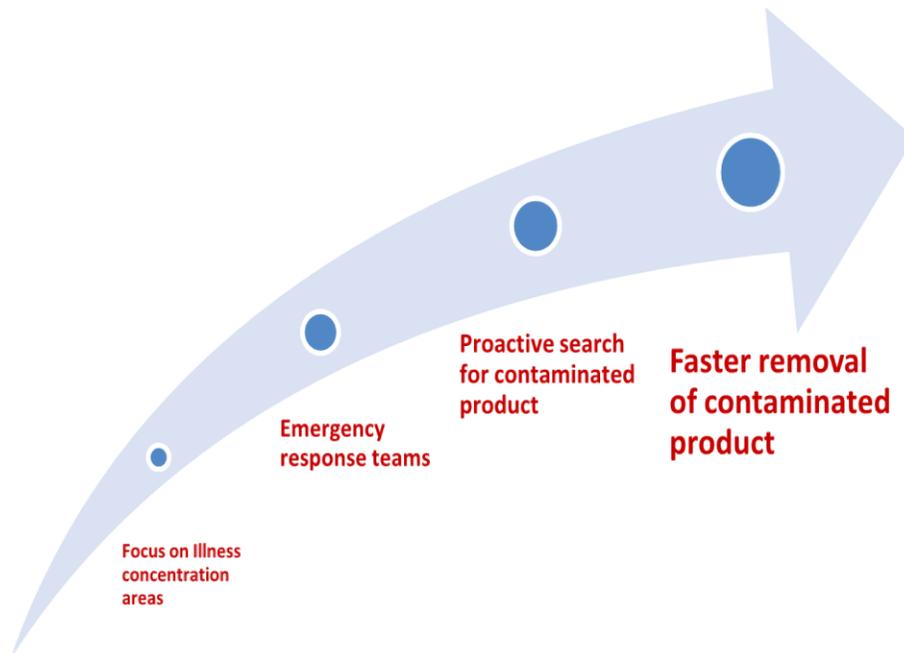
Critical Node	Mitigation Value	Criteria
Monitor student research	0.25	Some mitigation value based on actions to more effectively scrutinize student research in the future.
Strong intelligence	0.25	Some mitigation value based on actions to strengthen intelligence collection efforts.
Strong border controls	0.20	Some mitigation value based on actions to strengthen visa process.
Tamper resistant containers	0.95	Tamper indicating containers would be essential to restoring public confidence in [deleted] products.
Store surveillance "in and out"	0.90	Increased surveillance of food products is essential to re-building public confidence.
Pre-coordination with FDA	0.85	Close coordination with FDA would play an important role in confidence building.
Media plan	0.85	Effective media engagement is critical to re-building public confidence and protecting brand name.
Shareholder contingency plan	0.85	Board actions can affect stock values.
Emergency Response Teams	0.80	Public knowledge of effective response options can affect public confidence.
Product re-stocking plans	0.80	Product re-stocking is critical to recovery.
Illness concentration areas	0.75	The ability of [deleted] emergency response teams to detect poisoning can affect public confidence.
Removal of tampered containers	0.75	The ability of [deleted] emergency response teams to detect poisoning can affect public confidence.
Identify contaminated product	0.75	The ability of [deleted] emergency response teams to detect poisoning can affect public confidence.
Localized product recalls	0.70	Removal of contaminated product can limit the spread of illness and reduce consequences.

Indicators and Warnings

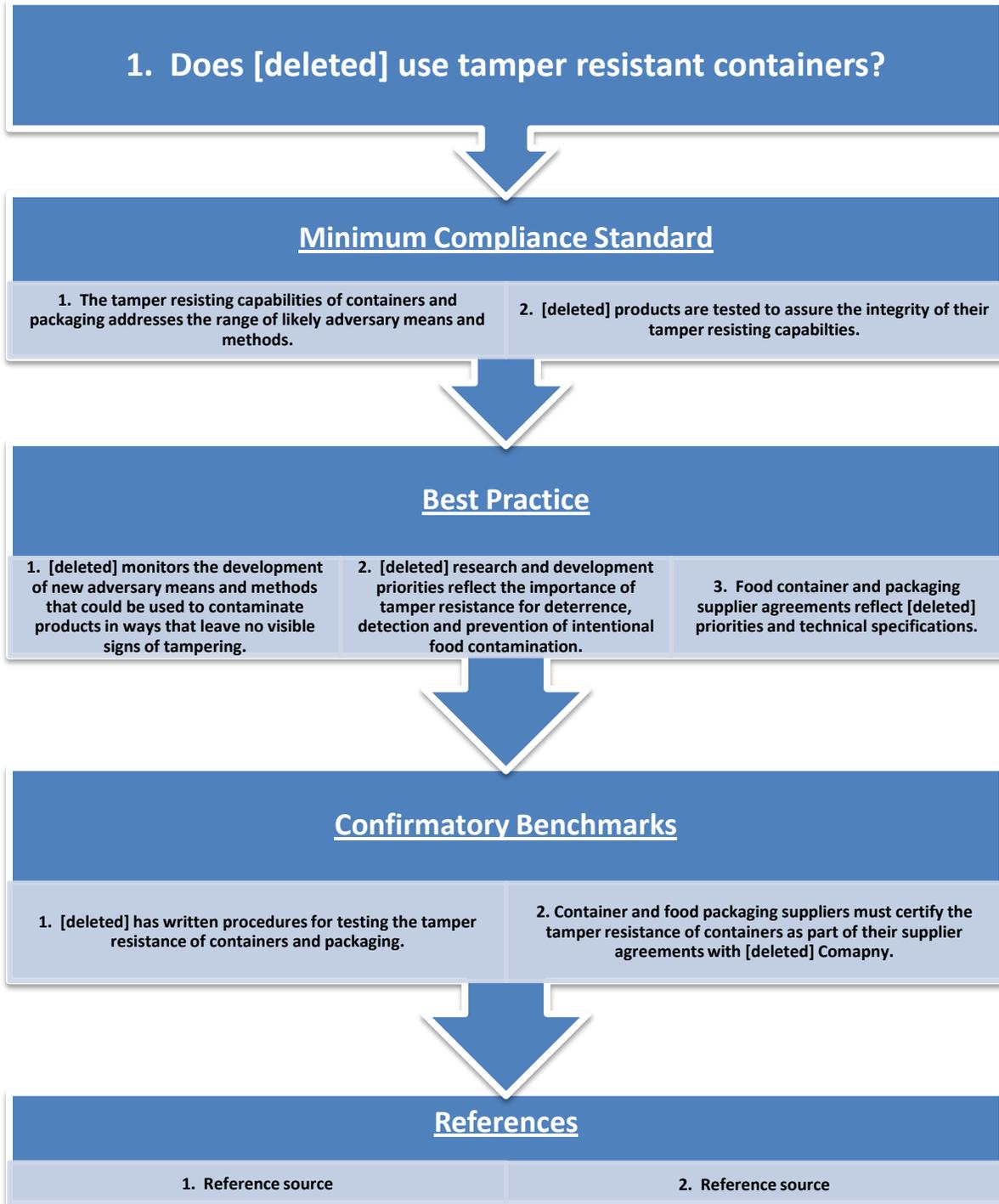
What information had it been known before the attack could have prevented it?



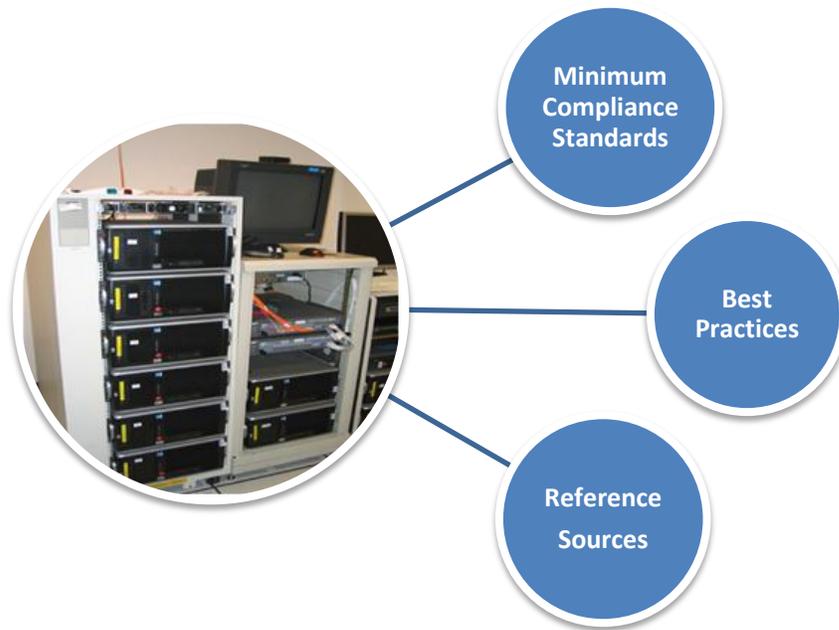
What information had it been known before the attack could have prevented its' escalation?



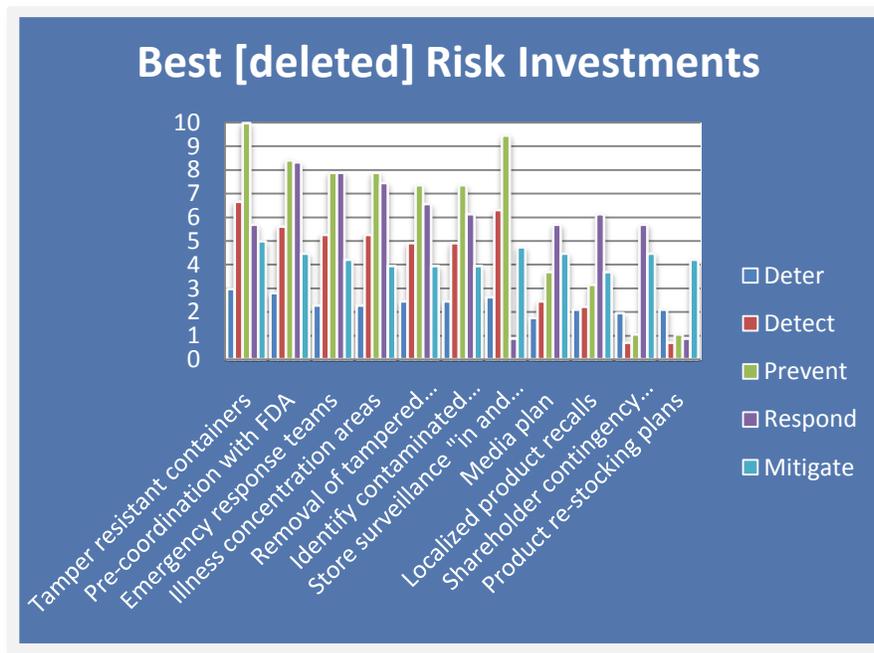
Data Sets for Each Critical Node



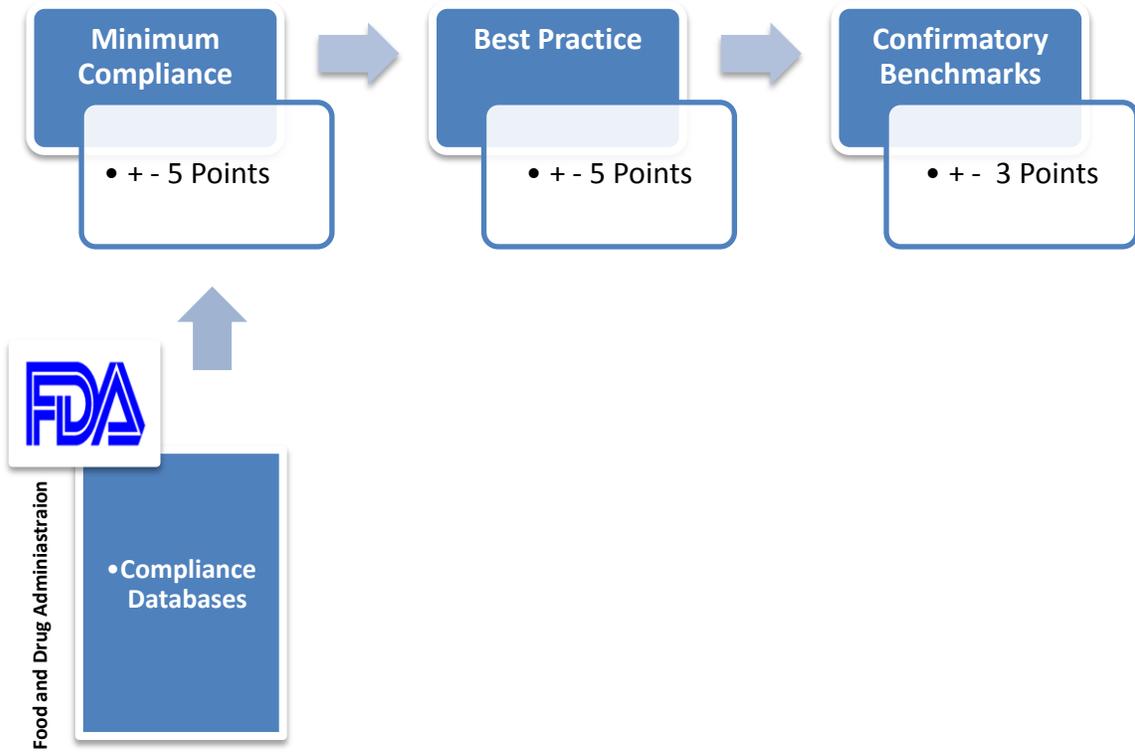
CSM Method® Knowledge Engines



Best [deleted] Risk Investments Based on this Scenario



Performance Assessment



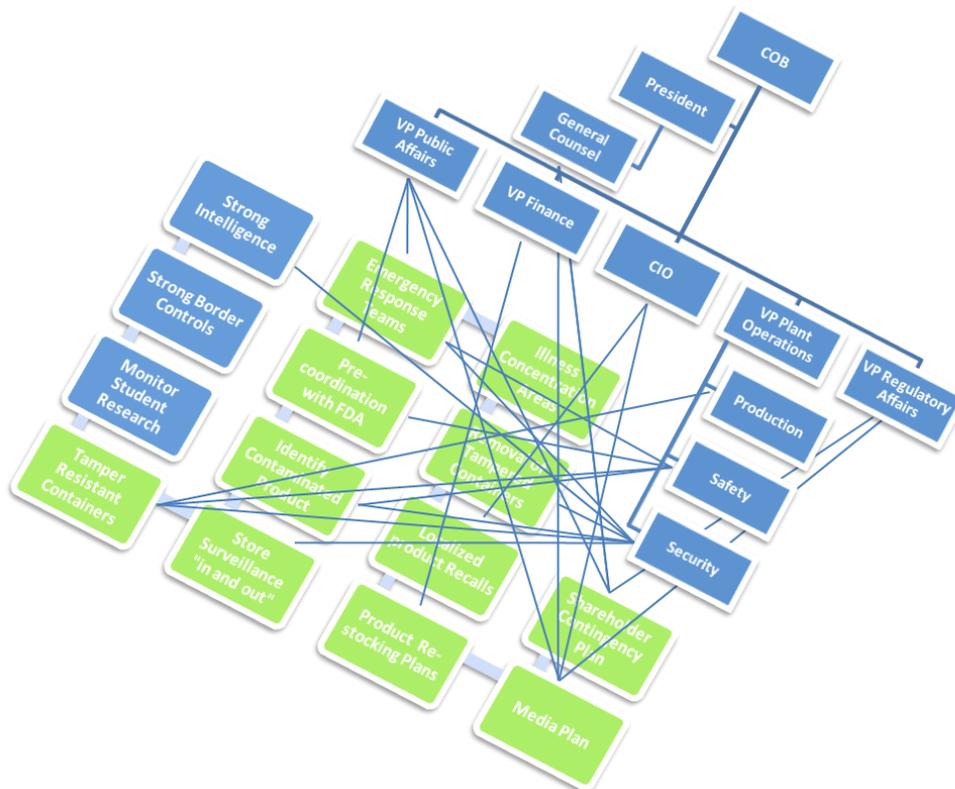
Graded Scores to Produce Threat Quotients



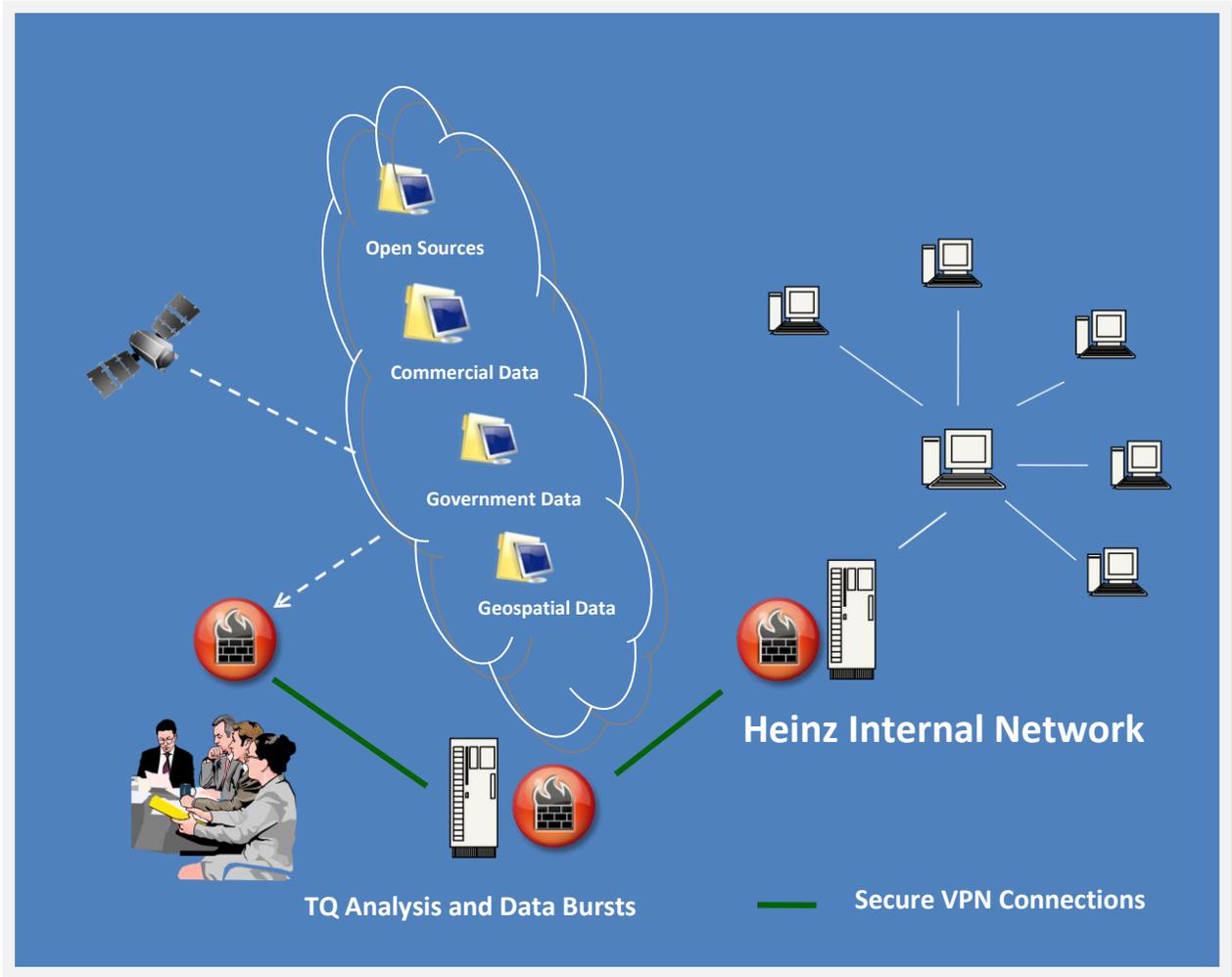
Continuous Performance Assurance



Organizational Mapping



The TQ™ Network



Outputs and Benefits

