Fall 2020 Role-Play Scenario

The product for ICSC 2020 is ReliaQuest's GreyMatter. The entire role-play competition is based upon a potential sale to DLL, the world's leading vendor finance partner.

Rounds 1A and 1B – Needs Identification sales meeting based upon a lead developed after receiving a tip from a fellow intern. Thursday (15 minutes).

Wild-Card Rounds WC-A and WC–B – Needs Identification sales meeting (repeat of Round 1 to the initial contact). Thursday (15 minutes).

Round 2, Round 3 and Round 4 (the Final Round) are a succession of meetings to completely define the needs of the prospect and seek a final "buy" decision. Friday/Saturday (20 minutes).

At the end of the Wild-Card Round, Round 2 and Round 3, a document will be released that summarizes the facts and needs that should have been uncovered in that round. This will allow all competitors moving on to the next round to start from the same point of reference.

Important Note to Competitors and Coaches:

ICSC attempts to provide as realistic a role-play situation as possible. Similar to a real selling situation, the sales person needs to learn about the product being sold, learn about the individuals in the meetings, learn about the prospect's company and even that company's customers. In addition, all ICSC role-play situations take place on a world-stage, so a basic understanding of current world events is always helpful.

Acknowledgements:

Thank you to all of the sales program faculty from around the world that continue to provide advice, encouragement and support as the International Collegiate Sales Competition evolves. Thank you to the sales faculty who shared ideas on how to run a sales competition online. And a special thanks to the faculty and staff of Kennesaw State University for sharing methods and ideas on how to run a large-scale collegiate sales competition; especially, Terry Loe, Director, Mary Foster, and Randy Stuart (Sarge).

Round 1:

In the summer between your junior and senior year, you and several of your classmates did an online internship with DLL. You loved the company and learned a lot about selling in an online environment. At the end of the internship, you and several others where offered jobs after graduation. It was a struggle, but you chose Reliaquest because technology just seemed to fit you better.

Your first year working for ReliaQuest has been very successful despite the Coronavirus pandemic. In fact, the pandemic has only increased the need for data security as many companies now have employees working from home. ReliaQuest constantly receives inquiries about GreyMatter because it greatly improves visibility across all cyber security technologies. It has been a changed world with almost all of your selling taking place online. You have learned lots of ways to engage a prospect and you have become a trusted consultant standing in front of a screen. Two years ago, you could not have imagined this would be the beginning of your career AND that you would find it both challenging and enjoyable in great part due to your internship with DLL.

You kept in touch with your fellow DLL interns, and one day Veronica Marin sent you a text that said "Call me right away!" In the ensuing conversation, Veronica told you about the possibility of DLL looking at new security technology because of something happening in Australia.

The Garvan Institute of Medical Research (https://www.garvan.org.au/) has been working on improved coronavirus vaccines and much of their equipment is financed through DLL. Although most of the actual science is conducted in labs, most of the support functions including accounting is conducted by Garvan employees at home. These are people who conduct business with DLL online. After a news story about a new potential DNA modification vaccine, DLL started seeing a 100-fold increase in intrusion alerts. Marin explained they just cannot investigate all the hits and would need to more than double their security staff for just this one account.

Veronica helped you by introducing you in an email to the DLL Program Manager that oversees Garvan, John (or Jane) Plantier. Veronica said that several top executives told John (Jane) that even though this was a very profitable account, they may have to cut the ties because the security people simply could not keep up with the huge number of intrusion attempts and that it could jeopardize their entire business. In a series of emails, John (Jane) agreed to a 15-minute meeting to find out about GreyMatter. And if it held any promise of saving this account, he (she) would introduce you to his (her) friend who will be involved in the decision. A Zoom meeting was set for the morning of Thursday, November 12th. Before meeting, you learned more about John (Jane) at https://www.linkedin.com/in/john-plantier-598a2713/.

Wild-Card Round:

"DO-OVER"

(Note – For the Wild-Card Round, please use all the information provided in this document above for Round 1. However, NO facts, needs, problems or references to any person or activity that was uncovered by any competitor during Round 1 of the competition is applicable to this Wild-Card Round.)

Ten minutes before the Zoom meeting was supposed to start, John (or Jane) Plantier sent an email apologizing for being unavailable and asked that the meeting be postponed to the afternoon after 2 pm. You replied with a few available times and he (she) picked one. You immediately sent a Zoom invite for the new afternoon meeting time.

Round 2 (20 minutes):

Setup for the meeting with Michael Godfrey

Note: Whatever you uncovered in Round 1 and/or the Wild-Card Round that does not agree with the following, please disregard. Below is what actually happened in the previous meeting.

John Plantier told you that DLL's association with the Garvan Institute of Medical Research has greatly increased the number of security incidents that DLL is having to investigate. John thinks there is a real concern that this may only be the beginning and that the attacks could get much worse. So, John thinks there is a struggle at DLL as to whether to hold on to the Garvan account or cut ties with Garvan in order to protect the security of DLL and its many other customers worldwide.

John did not know much about DLL's data security, as that is not his area of expertise. John was sure an outside company is involved, and John mentioned that there are many people in DLL who are constantly investigating every possible security incident. John also said that data security is important to many customers. Companies that have just one data breach lose a lot of customers. DLL has not experienced a significant breach and John wants to keep it that way.

John's interest is to continue to maintain accounts and even grow in the healthcare sector. In fact, if DLL could prove to be a more secure option, perhaps the result could be acquiring new business in both the healthcare and clean technology industries. John thinks that the better option is to enhance DLL's security and try to grow despite these new cyber-attacks.

John mentioned that others at DLL have talked about doubling the security staff that investigates incidents, and that would cost more than a half-million dollars—he thinks. Jon admits that this cost would not affect his budget, but he thinks that DLL should pay whatever it takes (within reason) to be more secure.

You convinced John that ReliaQuest could help to make DLL more secure. So, John set up a Zoom meeting with Michael (Michelle) Godfrey who is the Service Delivery Lead, Security & Connectivity, for DLL on Friday morning. John said that any solution would have to pass before Michael (Michelle) if it were to go any further. Before your Zoom meeting, you researched Michael (Michelle) at https://www.linkedin.com/in/michael-godfrey/.

Round 3 (20 minutes):

Setup for the meeting with Laura Whitt-Winyard

Note: Whatever you uncovered in Round 2 and/or the previous rounds that does not agree with the following, please disregard. Below is what actually happened in the previous meeting.

Michael Godfrey is not sure if these attacks are just malicious individuals attempting to disrupt the search for a cure or if these cybercriminals just think that medicine is where the money will be for the taking, but several medical organizations in Australia have been seeing an increase in suspicious activity. Michael wonders if this malicious activity will spread globally. One thing is for certain—DLL is having trouble in Australia.

Michael is concerned about DLL's Australian customers and their satisfaction because downtime is causing service disruptions. In the last three weeks, DLL shut down the identity and access management system to prevent possible unauthorized infiltration. There were 7 days with downtime with 4 hours being the longest one. This creates customer doubts and has the potential to impact DLL's reputation.

Michael has a team of 10 people dedicated to Australia who are analyzing every threat to determine its validity. DLL works with an MSSP, which has been feeding Michael's Australian team with dozens of incidents a day. The team is frantically trying to keep up with investigating these incidents and it is costing a TON in overtime. Michael did not feel comfortable disclosing the specific amount that overtime is costing him, but he does want to hire more personnel to handle the ongoing cyber threats in Australia. However, Michael is not optimistic about his request to hire 10 more people at an average of $75,000 each.

In Australia, DLL has a lot of hardware and software for security purposes, but DLL also uses an MSSP (the identity of which Michael did not want to disclose). That presented another issue. The issue Michael is having with the MSSP is compliance. Essentially, using an MSSP means that DLL is not fully able to report on compliance as some security functions are performed by the MSSP (an outside 3rd party).

You also asked Michael for specifics regarding the equipment he would want protected by GreyMatter in order to work up pricing. Michael indicated that Australia was an

immediate priority and wanted to see those numbers first. He agreed to email you those specifics.

You communicated several benefits of using ReliaQuest's GreyMatter and felt that handled Michael's concerns well. So, you pressed on for a meeting with the CISO of DLL, Laura (Larry) Whitt-Winyard. She (he) was fortunately available this afternoon, so a Zoom meeting was set quickly. In order to be prepared, you quickly looked Laura (Larry) up on LinkedIn at: https://www.linkedin.com/in/laurawhittwinyard/.

Michael's email contained a lot of information, so you figured you needed to at least have an estimate of what GreyMatter might cost DLL in Australia in case Laura (Larry) wants to know. So, from numbers you received in Michael's email, you came up with the following before your meeting with Laura (Larry).

Item	Category	Number	Unit Cost	Total	Notes
Network Servers dedicated to Australia	Integrated	25	$5,000.00	$125,000.00	Primary network in Sydney, Australia
Network Servers Parallel Backup #1	Integrated	25	$5,000.00	$125,000.00	Melbourne backup location
Network Servers Parallel Backup #2	Integrated	25	$5,000.00	$125,000.00	Brisbane backup location
SIEM Systems	Integrated	3	$5,000.00	$15,000.00	One at each site
Firewalls, filters, email security	Supported	50	$23.50	$1,175.00	Security for various locations/systems
Workstations and mibile devices	Supported	478	$23.50	$11,233.00	Desktops, laptops, tablets, phones
Security Users in Australia	Security Staff	15	$1,000.00	$15,000.00	5 System - 10 Incident Response Team
Other Users in Australia	Supported	324	$23.50	$7,614.00	Both DLL and client users

Round 4 (20 minutes):

Setup for the meeting with Laura Whitt-Winyard and
Bill (Billie) Stephenson (the role of Bill will be played by a female—hence Billie)

Note: Whatever you uncovered in Round 3 and/or the previous rounds that does not agree with the following, please disregard. Below is what actually happened in the previous meeting.

See the LinkedIn Profile for Laura at: https://www.linkedin.com/in/laurawhittwinyard/
See the LinkedIn Profile for Bill (Billie) at: https://www.linkedin.com/in/william-f-stephenson-26473422/

You met with Laura Whitt-Winyard, the CISO of DLL, who liked ReliaQuest's GreyMatter solution and wants to implement it in Australia. You received some info earlier regarding the hardware, software and personnel that would need to be monitored by GreyMatter so that a price could be determined. The total was over $425,000, but the investment in ReliaQuest is cheaper and more effective than hiring 10 more personnel at the cost of $750,000. Most of DLL's security team does not have expertise in the specific intrusion attempts that are currently being launched in Australia. And, only half of them are experts in the specific antivirus and SIEM systems in Australia. Recruiting more people with the specific talents required may take a lot of time. By the time they are recruited, it may be too late to prevent a serious breach. DLL could quickly relocate employees from elsewhere to assist (which will leave other regions vulnerable).

In addition to attacks on DLL through the Garvan Institute of Medical Research in Australia, a few other clients in the medical industry (and related industries) in Australia that have begun to generate many more alerts for DLL. The volume of incidents that merit investigation is increasing far beyond the staff that is dedicated to Australia. The MSSP (Managed Security Service Provider) DLL is using in Australia has been feeding the Incident Response Team with dozens of cases per day. Once investigated, it seems that many of the incidents are recurring, harmless events. Thus, the response team is wasting time on these incidents when they could be investigating some of the more worthwhile (and more sinister) intrusion incidents. The MSSP claims that the variety of hardware and software in DLL's Australia network is the reason the same incidents are being reported as unique occurrences. However, there are real threats that end up waiting in a que to be investigated. ReliaQuest specializes in determining what is critical from what is trivial, thus allowing the existing team to work more efficiently to manage the incidents.

Laura (DLL's CISO) asked you to send her a contract that must pass before DLL's legal team before being signed. She said she would sign and return the contract within 24-hours. However, you received an email from Bill (Billie) Stephenson, the CEO of DLL. Bill (Billie) asked to meet with both you and Laura because there were some questions that needed to be answered before DLL would move forward with ReliaQuest. In essence, Bill (Billie) still needs some convincing before saying yes.