###### Comm 1116 Incident Report Practice

You work for International Computing Machines (ICM), a network consulting firm that sets up and maintains networks for mid-sized and, more recently, large companies and institutions. You are their Network Security Analyst in Vancouver. One morning, at 10:30am, the ICM Associate Director of Network Security, Ang Lee, comes into your office to talk to you. The conversation is as follows:

Ang: Pack your bags, you’re flying to Victoria.

You: Are you kidding me?

Ang: Nope. Well, you won’t have time to pack, because you’ve already been booked to fly out on the Helijet in an hour, at eleven thirty.

You: The Helijet! What’s happening in Victoria that I need to take a helicopter over there? Isn’t that expensive?

Ang: You bet. $428 for a return ticket, plus taxes. And you might have to stay there overnight if the problem can’t be fixed right away. Maybe longer if necessary. But it’s all on the company credit card, so just pay and get the situation fixed. The problem is at the government offices in the Department of Human Services, one of our newer but larger clients. They say they’re under attack. The DHS is being hacked! This is an important client so needs fixing.

You: Hack? Attack? Who’s attacking them? And why?

Ang: They don’t know. Could be anybody. All they know is a bunch of their computers seem to have been compromised from outside. Their Victoria Network Administrator, Sissy Spacek, called me ten minutes ago and reported finding some malware in at least one computer, and when she ran a security protocol she got some super-high data feed readings from the network interface cards on a bunch of computers, as if someone outside the company somewhere on the internet was downloading a lot of company data. Secure, personal data.

You: Wow. The DHS must have reams of confidential data on millions of people, everything from Social Insurance Numbers to tax records. They store information from employment insurance, student loans, and pensions, just to name a few. Big information.

Ang: Exactly. That’s why they’re freaking out over there, and that’s why we need to send you over by helicopter.

You: Do they know what information was downloaded or taken?

Ang: No clue. All they know is that a lot of computers were compromised. Sissy just found out all this at about 10:00 this morning, and she took all the compromised computers offline right away, but the damage may already have been done. Then she called us after that.

You: That’s weird; all those computers are protected by Symantec Norton anti-virus and firewall. The hackers must have found some new bug or exploit to get past Symantec Norton like that. Not that it’s too difficult what with the multiple access points – laptops, phones, cloud systems – that modern institutes use for work.

Ang: Well, you’ll need to find out what the threat is and fix it, fast. Better get going for the Helijet!

You take the 11:30 Helijet from downtown Vancouver to downtown Victoria. The sky is clear, and visibility is good all the way across the Georgia Strait. The flight takes only 35 minutes. You catch a cab to the DHS; it cost $20 (tip included), so you put it on your company credit card — like everything else you need to pay for in Victoria. You love using the company credit card for everything; it’s a great perk but is very necessary too when you take last-minute work trips like this.

When you get to the DHS offices ten minutes later, you talk to Sissy Spacek:

Sissy: This morning, at around 9:45, one of our office managers was browsing local government websites and got a warning from Symantec Norton about some malware detected, so he called me to ask me about it. I thought it wasn’t a big deal, but then I ran the Symantec security protocol, and it flagged thirteen of our brand new computers as having a lot of data being sent out onto the net. We have so much sensitive data on these computers. I couldn’t even tell what was taken or where it was going, so whoever was doing it knew how to cover their tracks. We’re all very upset about it. My bosses are not happy.

You: We’ll focus on the bosses at a later time. What did Symantec Norton tell you about the malware? And how much data was downloaded?

Sissy: Symantec Norton said it detected two malware objects in the Explorer browser cache. Both objects were inert, and both were quarantined and deleted. Symantec Norton said they were Threat Level One. I’m not sure how much data was downloaded. The scan results seem inconsistent.

You: Well Threat Level One is the least serious level, not the most. It means the network wasn’t compromised. Also, because Symantec Norton blocked any malware activity, I suspect this malware may be unrelated to your network breach and data theft. I'd better take a look at those computers.

You spend the next three hours trying to find what information was downloaded from the affected computers - and how - but you can’t find anything. You run initial system scans at 12:30, but they don’t tell you what data had been downloaded. Weirdly, they don’t show any large downloads having taken place from outside. It doesn’t seem like anyone has penetrated the Norton firewall and compromised these computers.

At 3:00 pm you almost give up – you can’t quite figure the solution – and go to the hotel across the street, paid for by the company. As you’re walking back to the hotel, an idea occurs to you, so you turn around try it out as soon as you get back inside DHS. You discover a solution to your problem. The walk helped! You call your boss at 3:45 PM and tell him about it:

You: I solved our problem. For now.

Ang: That’s great, I knew you could do it! What did you do?

You: I kept getting high data output readings from the network cards, but other security scans didn’t support those readings, so I swapped out the network card on one of the compromised computers. I swapped it with a network card from a computer that I knew was secure. Sure enough, the compromised computer suddenly gave the same readings as a secure computer. And the secure computer suddenly started showing unusual amounts of data going out.

Ang: It’s the network cards!

You: That’s right, it’s the network interface cards. They’re the initial problem.

Ang: What did you do?

You: I figured it’s some kind of firmware glitch on the cards that produces faulty I/O readings, so I got a network technician to start taking out the cards. All thirteen cards with problems are part of the rollout of twenty new computers that were installed two months ago at the DHS. The other seven computers seem fine, but I’m having those cards swapped too. There definitely seems to be some kind of factory defect going on with these cards, so I won’t take any chances. I called our supplier to deliver some replacement cards immediately, and they’ll be here this evening, by 5. They should all be replaced and everything back online by 7.

Ang: They’re not going to charge us, are they?

You: Hell no! We should charge them. It’s a straight exchange, no charge. They just found out a known issue that these cards have caused a problem, and they’re very apologetic. They would have been in touch tomorrow morning to report it to us and send us new NIC cards.

Ang: OK. Well, thankfully this issue is solved. Great work. When are you coming back?

You: I’m catching the six o’clock Helijet back. Sissy Spacek can take care of getting these computers fixed and back online. Sissy's very good at her job; she just made a natural mistake when she assumed a security breach, and it’s safer to assume the worst as she did. But I wouldn’t say it’s *all* solved…anything but…

Ang: You mean the overall security at DHS?

You: It’s time for a major upgrade. We shouldn’t have to fly out to fix urgent issues; security has to become more centralized so we can fix from any location. And with such sensitive data, all government agencies such as DHS need to move into a much higher bracket of security than the small business level server products currently used. DHS has waited for too long to upgrade, but with multiple OSs used by employees, use of the cloud for storage, and mobile devices used for work in government, the time for upgrade is now. At the latest. This event was a perfect prompt to show DHS that security cannot be compromised. Cost is not a factor here. They’re lucky this time.

Ang: Absolutely. Symantec’s new Integrated Cyber Defense System is a great example of a modern, robust system that could be implemented at the government level. Its threat protection and information protection are extremely solid. Other companies have similar software that can be equally effective, but we are used to working with Symantec products; they’re highly effective. The cyber threats are so big for government agencies, so they have to up their game to meet the new threats of information theft and security.

You: Agreed. They’ve got to have systems in place where people such as myself can control everything from my base, wherever that is. And they’ve got to have cyber security that covers all devices, OSs, cloud based systems, anything and everything that is used by employees that has potential access to private data. We’ve moved to a new level of cyber threat and have got to get companies to understand the challenges faced.

Ang: At least the money we spent getting you over there this time was well spent. It could have cost us, and them, lots more if the issue had been bigger. With all the ransomware on the Internet, security is more important than ever. As you say, it’s a wake-up call for the DHS. I’ll contact their CEO and COO, Brianna DeWit and Kele Ihenacho on a conference call now. They need to know what happened. We’ve got to prevent bigger incidents in the future and get them to upgrade right away.

You: OK, let me know what they say.

Only a short time passes before Ang calls you again.

Ang: Get the report written asap tomorrow. Send it to me, Brianna, and Kele. DHS agreed to our solutions for upgrade.

You: Everything we said needs to be done, they’ll pay for and we’ll implement?

Ang: Yup. The new CEO and COO realize the need for change and trust us to make those changes. That’s why they hired us, and that’s why we hired you; your technical skills sorted this mess out, and your communicative competence will make the report as clear as water.

You: Thanks boss. That helicopter was a sweet ride by the way. The way it handled and the……….

Ang: Write the report brains. See you tomorrow. You’ve earned a night at that hotel.

Write the incident report in a Word document.

Format it based on the lecture files and features from the book.

Don’t copy the language used above; much of it consists of casual conversation and may contain errors.

Consider who you are writing to and what they need to know in the report.

Use the checklist on the next page as a guide.

Here’s a link to the Symantec Integrated Cyber Defense concept, for your information:

<https://www.symantec.com/theme/integrated-cyber-defense>

###### Incident Report Marking Criteria

##### Content and Organization

* Identifies incident, times, and dates
* Appropriately organizes information (Summary, Timeline, Root Cause, Resolution and Recovery, Corrective and Preventative Measures)
* Provides details regarding:
  + The incident
  + The root cause
  + What remains to be done
  + What will be changed or needs to be changed
* Focuses on the specific reader needs

**Presentation**

* Correct report format and structure
* Informative and self-explanatory title
* Appropriate headings
* Appropriate paragraphing
* List format where necessary
* Appropriate use of white space

**Style and Grammar – Edit and Proofread**

* Objective, concrete, specific language
* Direct, clear and concise language
* Complete sentences
* Appropriate punctuation
* Correct verb tenses
* Subject/verb agreement
* Articles
* Plurals
* Word choice
* Words missing
* Correct hyphenation
* Awkward phrasing