TUCK SCHOOL OF BUSINESS AT DARTMOUTH
GLASSMEYER/MCNAMEE CENTER FOR DIGITAL STRATEGIES
VINCENT L. LACORTE CASE SERIES

Case #6-0029

Making Information Risk Mitigation Decisions

Part A

The Setting

Mary Cartwright was sitting in her office at Jefford's, a Fortune 500 company that designs, manufactures and sells all manner of thermostats and more sophisticated electronic controls for managing energy consumption in buildings. She was puzzling over how to attack a variety of information security challenges the corporation was facing, most specifically over what investment and policy changes she should propose for the next fiscal year to address the challenges. In a month's time she was scheduled to brief the management team and later the board on the investments she felt were necessary in information security to put the organization in the proper position going forward. Everyone was aware that protecting intellectual property was increasingly a challenge, and, because of the nature of Jefford's business, increasingly important.

Mary, Jefford's head of information security, started her planning by thinking about the last year's information security events. In the past year, Jefford's had suffered 48 reported and verified information security incidents, most of which involved stolen or lost laptops or handheld devices. Interestingly though, Mary did not think those stolen or lost devices represented the most serious of the incidents, though a couple were close and Mary felt strongly that she would have to address the laptop issue. The most serious were five separate incidents of virus outbreaks, four of which were shown to have been the result of unpatched workstations and/or servers; the other one resulted from an infected laptop brought in by an employee being connected to the intranet behind the firewall. Three of the malware events brought supplier logistics servers to their knees for periods ranging from 4 to 19 hours, and one had affected distribution pretty severely, halting shipments from their warehouse in the southeastern U.S. for nearly an entire day. The malware from the infected laptop corrupted the sales database erasing a number of files that had to be painstakingly rebuilt. There had also been indications of a targeted attack against Jefford's servers likely originating from China.

This case was written by Professors Hans Brechbühl and Stephen Powell of the Tuck School of Business at Dartmouth, Chris Dunning of Staples, and Center for Digital Strategies Senior Research Fellow Scott Dynes. The authors would like to acknowledge the contributions of Phil Venables of Goldman Sachs and Larry Ponemon of the Ponemon Institute. Note: With the exception of the Appendix (actual data), this is a fictional case study. The names, companies, and facts used here are not real and do not represent any individual or company. This case was written as a basis for class discussion and not to illustrate effective or ineffective management practices. Version: May 2008.

Mary was also aware of a recent incident in a smaller company in a neighboring industry that had temporarily paralyzed the company in which it occurred. This other company's network had been compromised and their human resource database accessed, resulting in the theft of the names, addresses, birthdates and social security numbers of 3,000 of the company's employees. Needless to say, the loss in productivity among employees over the weeks that followed the discovery, the days of executive-level time dealing with the issue internally and externally, and the cost of the fraud monitoring service the company had subsequently bought for each of the affected employees was substantial. Mary was concerned that they might not have the right precautions in place to prevent a similar breach of personal identifiable information (PII) from happening to Jefford's at some point as well. Jefford's had outsourced much of its HR data processing, and Mary was concerned about the potential of a security breach at one of these vendors.

Jefford's has an online B2B site where wholesalers, distributors and retailers place their orders and through which they are able to track the fulfillment process. While the websites had never been brought down in the prior year, both the corporate site and, especially, the transaction/sales site, were constantly under attack, with thousands of attempts to improperly access the site on a daily basis. But the real concern regarding the B2B site in Mary's eyes was the growing evidence of fraudulent transactions in this channel. As recently as four months ago, online fraud had been below 0.15% of sales and not really a worry—it was simply treated as a cost of doing business. But the fraud percentage was now approaching 0.30% and Mary was concerned that the trajectory was not good. As the business grew and spread geographically, the problem was clearly growing and would eat into the 9% margin the company enjoyed.

The Company

Jefford's sales last year were just over $5 billion and growing rapidly, largely fueled by the continued retrofitting of commercial buildings to make them more energy efficient, as well as skyrocketing oil prices that had made all customers including consumers more concerned about what they were spending on heating their buildings. Sales were also benefitting from the commercial building booms in Russia and China. Jefford's has various levels of products, some industrial strength and some more modest systems for high-end housing, but almost all designed for automated and/or even remote management.

Though Jefford's was the market leader, their two chief competitors were close to them and also growing rapidly. One was a Canadian company that had grown with Jefford's, the other a Chinese company that was a newer entrant and was rapidly gaining market share. The Chinese company had been a 50-50 joint-venture started with one of Jefford's domestic competitors, but the Chinese company had bought out the American company about 18 months ago. Jefford's too has some production in China and their partner has a poor relationship with their chief Chinese competitor who appears to have a close relationship with elements in the Chinese military.

About a third of Jefford's sales were now online. This was a rapidly growing part of their business, but Jefford's sales force was a historically significant and still very important part of their approach. While the sales force in the continental U.S. numbered about 900 people,

Jefford's had wholly or majority-owned subsidiaries strategically placed in other countries throughout the world, particularly in Europe, Latin America, the Middle East, and Russia, though their leadership was largely American and the headquarters was in the U.S. and most of the shipping was still out of the U.S. as well. Jefford's had about 30,000 employees. In various places in the world they sold through wholesalers, other distributors, and, in the case of their consumer products, sometimes directly to retailers. Since much of the most recent growth in size of the company had come through a set of relatively new acquisitions, Mary was admittedly less familiar with operations outside the U.S. It seemed unlikely that the pace of acquisitions would slow down anytime soon.

The Challenge

Logistics, intellectual property protection, reputation with customers, the ability to transact business over the B2B sites, daily logistics operations, protection of personnel data—each depended in a critical way on Jefford's information infrastructure, and Mary's ability to manage the risk to the information held and conveyed by that infrastructure. She knew she would have to be effective at rationally evaluating the likelihood and impact of events, and balancing that against the cost and effectiveness of mitigating strategies. Mary knew that there were many projects at Jefford's looking for funding, and not just information technology (IT) projects. She also knew that to be effective at the job, she would have to be effective at convincing the board, which included being able to concisely explain the process that she used to arrive at her recommendations. But first she had to figure out what the real issues were, gather some data, and decide what she thought it best to recommend.

Part B

It was two weeks later, and Mary was beginning to piece together the picture on the various security issues she had been thinking about. She now wanted to sit down and analyze the inputs she was receiving and start drafting a set of recommendations and the slides for her presentation.

She had asked one of her direct reports to research the costs of laptop encryption and another to look into potential solutions to the ever increasing web fraud issues. She had just received both reports this morning. Mary had herself done the research into what steps to take to mitigate future malware issues. While data on employee PII loss and its ramifications had been hard to come by, Mary found out from Jefford's privacy officer that Jefford's was part of a group of companies that met periodically with Larry Ponemon of the Ponemon Institute. Larry's organization conducts independent research as part of its mission of "advancing responsible information and privacy management practices in business and government," and since Jefford's was a member of the group, Mary was able to get the most recent composite data on the expenses incurred as a result of employee data breaches in nine Fortune 500 companies in 2007 (see Appendix). A brief summary or discussion of each of the four areas of concern follows.

Laptop Encryption

Jefford's has 4,500 laptops in the hands of their employees at present. The approximate breakdown is: 2,350 sales force laptops; 650 engineer/R&D laptops; and 1,500 executive/ management laptops. The consequences of compromise were not the same for each type, nor was the likelihood of loss. Sales force laptops have sales data, product information, and sales leads or customer data on them—if compromised, the average cost for a single laptop was estimated to be $500,000 and the likelihood of a loss 2% of laptops per year. Engineers have product development data and energy-management algorithms on their laptops, which, if compromised, could jeopardize Jefford's presumed development lead on a vital stream of new products, leading to an average loss estimate of $5 million per laptop, but a loss likelihood of 0.5% of laptops per year. Executive laptops have corporate strategy, as well as sales goals and partner information on them, and, in addition, some contain employee PII. The cost of a compromise was estimated to be $2 million per laptop, with a likelihood of loss of 0.7% of laptops per year. For all laptops, the likelihood of compromise of the data if a laptop was lost was small—about 1%.

Commercial encryption solutions range from $40-$140 per laptop depending on quality and how they were implemented. The more expensive solutions are indeed the better ones, and they made it more difficult (and expensive) for anyone to decrypt the laptop. Generally the better commercial solutions are considered 97% effective.

Malware Protection

It was hard to estimate the exact costs to the business of loss of systems. In the case of the supplier logistics servers brought down last year, it was clear that the resulting delays in arrival of component parts had idled at least one plant for one of two eight-hour shifts. The cost in salary paid to a shift that did not work was just over $170,000 without attributing any cost to the $85 million of capital equipment that lay idle. Even if there were no effects in sales losses downstream, that was a significant loss and certainly not sustainable for very long.

The estimates of what the distribution interruption cost the company also varied. Jefford's daily sales were about $20 million, of which 50% was in the U.S., 40% of which shipped out of the affected warehouse. The penalty for late arrival of a shipment was 1% of the value of the shipment, so the minimum cost of that disruption was $40K.

The company already invested the roughly $50/year/seat that it cost to maintain a solid enterprise anti-virus suite standard, though occasionally a laptop or two slipped through as was the case with the salesman's laptop that was not up-to-date (because he had accidentally disabled the anti-virus update prompt) and infected the sales database. The cost of that incident had been estimated at about $40,000 in direct costs of time and lost sales. In Mary's mind this was largely a matter of enforcing policy on sales people who were not in the office much and did not understand the importance of such "admin" procedures as anti-virus updating.

As Jefford's had grown rapidly over the last eighteen months, much of it by acquisition, server patching was still catching up to their growth, especially in the areas of the company that had been acquired. Many locations outside the U.S. and Western Europe were still patching manually, and Mary realized it was imperative to turn her separate U.S. and European licenses (for automated patching) into an enterprise-wide license and add a person to manage the patching of the other regions. Mary thought the conversion of the license would cost $50,000 annually and the additional headcount would probably cost $80,000. Widely available data shows that unpatched servers will be compromised with a probability of 80%. Patched, the odds are much lower.

Website Fraud Prevention

Mary's colleague had come back with two possible directions to take to reduce website fraud: implement two-factor authentication on the website for all customers, or invest seriously in a fraud prevention department and the software tools needed with it. (The existing fraud prevention effort was ad hoc and had not caught up with the rapid growth in web sales.) Jefford's B2B website was generally well liked by many of its customers for its ease of use. But the incidence of fraud had increased even further just in the last two weeks and was now 0.35% of sales over the web.

Discussions with colleagues in neighboring industries indicated that others were seeing increases in fraudulent transactions and many had already taken steps to address this. Mary's direct report had a colleague at a company he used to work for who heads web security for a

B2B site that does about $2.5 billion of business annually. They had started a small loss prevention group investing $75K in a software license for a solution named Clear Commerce and about $425K in annual personnel costs. He had confided that his company's return for this investment was pretty clear: while they still suffered about $4 million in losses due to fraud every year, it was clear that if it were not for their loss prevention focus, the losses could be up to 10 times as high. In the neighborhood of 0.15% was considered a "cost of doing business" and therefore accepted.

The research indicated that to add two-factor authentication to the site would cost about $500K, plus $20 for each of 6500 online customers. It would also, undoubtedly, cost Jefford's some customers, perhaps as much as 2.5% of its online revenue. But it was likely to be 99% effective.

Employee PII Protection

After seeing the Ponemon data, a group discussion with some of Mary's group, members of HR, and the privacy office, led Mary to believe that her concerns about PII protection efforts by third-party vendors were well-founded. Jefford's had never really gone beyond asking for self-assessments from its vendors of their efforts to control the risk of PII compromise. Given that, the group felt there was roughly a 5% chance of a breach during a year and that between 40% and 100% of their employees would be involved.

The group agreed that they had two options: they could make their "secure vendor" program much more robust, and/or they could add a data loss prevention tool (DLP) from a vendor like Vontu or Reconnex to their inventory of software services, and insist on its installation on the systems of their HR-related vendors as well, though they would likely have to pay for it. It seemed that a more robust and continuous "secure vendor" program could lower the probabilities of a large-scale breech by 20-40%, where a DLP tool would reduce risk by 80+%. The combination could be pretty powerful in protecting this critical area, but would be fairly costly too. Mary's initial inquiry into costs to implement led to an initial cost of about $500,000 for the DLP and about $300,000 for a robust "secure vendor" program for their HR vendors.

The Investment Question

With all these matters to consider and a limited budget, what should Mary be recommending and why?

Appendix: Cost of data breach involving the loss or theft of employee information

Analysis prepared by Dr. Larry Ponemon, April 30, 2008

The following tables summarize nine (9) activity-based cost accounting studies that involved the loss or theft of sensitive personal information about employees. Eight organizations are Fortune 500-sized corporations and one organization is a large U.S. federal agency. All participating organizations are located in the United States. The data collected or extrapolated below was collected in 2007 by Ponemon Institute based on confidential interviews with actual companies experiencing the data breach.

Table 1. Costs of Remediation by Cost Category. All numbers are expressed in U.S. dollars with $000 omitted. The cost figures are the total amounts or sums for all nine case studies.

Discovery cost ($000)	Direct	Indirect	Total
Forensics	$173.3	$139.7	$313.0
Internal audit	34.5	309.1	343.6
IT operations	17.2	1324.8	1342.0
Outside consultants & experts	290.8	34.5	325.3
Legal counsel	172.1	713.7	885.8
Administration	0.4	110.5	110.9
Other costs	19.9	22.4	42.3
Subtotal	$708.2	$2654.6	$3362.8

Escalation cost ($000)	Direct	Indirect	Total
Internal audit	$1.9	$225.8	$227.8
IT operations	19.9	164.7	184.6
Outside consultants & experts	300.8	2.4	303.2
Legal counsel	201.7	35.1	236.7
Incident response team	8.5	106.7	115.3
Other costs	26.8	18.4	45.2
Subtotal	$559.5	$553.3	$1112.8

Notification costs ($000)	Direct	Indirect	Total
Outbound communications	$3661.1	$1510.5	$5171.6
Inbound communications	605.7	342.9	948.6
Outside consultants & experts	458.5	17.3	475.8
Document management	98.0	3.2	101.2
Public relations	77.0	3.6	80.6
Corporate communications	3.7	137.1	140.8
Legal counsel	307.1	164.4	471.5
IT operations	31.5	7.8	39.3
Other costs	74.7	61.8	136.5
Subtotal	$5317.4	$2248.6	$7566.0

Ex-post response costs ($000)	Direct	Indirect	Total
Inbound communications	$2070.1	$1573.0	$3643.1
Public relations	95.1	627.0	722.1
Corporate communications	3.3	32.5	35.8
Outside consultants and experts	278.1	33.8	311.9
Free or subsidized services	4032.0	580.0	4612.0
Legal counsel	3089.3	208.1	3297.5
IT operations	32.5	25.3	57.8
Subtotal	$9600.6	$3079.6	$12,680.2

Employee impact costs [extrapolated] ($000)	Direct	Indirect	Total
Estimated absenteeism costs	$2152.9	$18,365.5	$20,518.4
Estimated lost productive time	26.5	4864.8	4891.3
Estimated turnover	648.6	2443.8	3092.4
Subtotal	$2828.0	$25,674.1	$28,502.1

Table 1 Totals ($000)	**$19,013.7**	**$34,210.1**	**$53,223.9**

Table 2. Case studies used in the analysis.

	Studies	Size of breach # of records
Financial	Case 1	1,792
Consulting	Case 2	36,000
Energy	Case 3	86,656
Pharma	Case 4	9,640
Retail	Case 5	8,190
Pharma	Case 6	27,349
Financial	Case 7	18,030
Telecom	Case 8	2,340
Government	Case 9	1,117
	Total	**191,114**

Table 3. Averages.

	Direct	Indirect	Total
Average costs per company experiencing the data breach ($000s)	$2,113	$3,801	$5,914
Average cost per victim (employee) ($s, NOT $000s))	$99	$179	$278