NED UNIVERSITY OF ENGINEERING AND TECHNOLOGY

MASTER OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

SPRING SEMESTER EXAMINATION -2010

Dated: 17-05-2010

Time: 3 Hours **Max Marks: 70**

INFORMATION SYSTEM AUDIT – CT- 532

Instructions:

- **Attempt all questions**
- **Read the case study thoroughly before attempting any questions**

1. What were the security issues encountered at Harland Clarke Holdings? Discuss [10]

2. What new measures were taken by the management to improve the security structure of the organization? [10]

3. What ten domains were identified by the security team to focus on? Explain any TWO domains in detail [10]

4. If you had been the security manager of Harland Clarke Holdings, what other measures would you have taken to increase the security in the organization? [10]

5. "Risk management is not a stagnant process but a continuous one". Explain the statement giving arguments and examples from real life scenarios. [15]

6. Explain in your own words, how the security implementation exercise was successful. What were the major success areas and what were the major differences between the structure of the organization before and after the implementation? How did it suit the needs of the people? [15]

Harland Clarke Rechecks Risk Management

New security program adds more systematic processes for evaluating, prioritizing and mitigating risk

Three and a half years ago, Harland Clarke Holdings' approach to security was very much in tune with its identity as a market-leading manufacturer of checks and check-related products for businesses and consumers. Security, according to John Petrie, chief information security officer at the San Antonio, Texas-based company, was a tactical concern that focused on the production processes in its nine plants throughout the U.S.

But that approach was becoming a bit old-fashioned as Harland Clarke expanded beyond its manufacturing roots, adding customer contact centers, direct response marketing services and electronic commerce capabilities to its offerings.

"There were issues around protecting electronic data, and our printing processes had changed over to the digital age,

so there was a transformation that had occurred," Petrie says. "We knew we had to change our risk management structure."

That's why, when Petrie was asked to join the company in 2004, Harland Clarke (named Clarke American at the time) was on the brink of a CEO-driven reinvention, not just of the processes it used to make security and risk management decisions but also the way its entire culture viewed security. In order to retain its competitive position in the market, "we wanted to become a secure provider of checks and check-related services, versus just a manufacturer," Petrie says.

Meanwhile, by 2005, Harland Clarke's own customers—financial institutions—were demanding more security controls and risk programs from their suppliers, thanks to regulatory changes that required them to prove end-to-end security in their supply chains.

Three Priorities

The top three priorities of the new security program, Petrie says, included taking advantage of enterprisewide quality processes (the company won a Malcolm Baldrige National Quality Award in 2001); linking security and risk mitigation decision processes to the business's operating plan and strategic growth goals; and ingraining security into the mind-set and daily activities of Harland Clarke's employees. "We wanted to make sure security wasn't a thing that sits out there and functions on its own," Petrie says.

It was essential, Petrie says, to leverage Harland Clarke's quality program in the design of the security program, especially to enjoy the cost savings. "We were able to take advantage of the solutions we implemented for quality in the areas of identification, notification and prevention," he says. For example, in each plant there are personnel in charge of monitoring and maintaining quality processes. Now those same people are also responsible for determining whether events that could potentially affect quality might also impact security, such as changes to plant schedules or machine malfunctions.

To reflect security's new central role in the business, the company also changed its organizational chart. Previously, security was a decentralized function that was governed by the CIO and the plant managers. Now, as CISO, Petrie reports not to the CIO but to the company's chief security officer, who also owns physical security and incident management. The CSO, Pat Patterson, who was a former FBI special agent in charge, reports to the senior vice president of administrative services (as do human resources, general counsel, the compliance officer, the privacy officer, partner support and partner reporting), who reports to the executive management team.

And to make security more of a business function, it was also important, Petrie says, to develop a program that was made up of repeatable, auditable and measurable processes. To that end, Harland Clarke chose a standard—ISO 17799/27001—that would serve as a baseline for developing its security controls and budgets. The standard stipulates 10 domains that define best practices for several areas, including business continuity planning; system access control; system development and maintenance; physical and environmental security; compliance; personnel security; security organization; computer and operations management; asset classification and control; and security policies. Each of these domains is also connected by governance guidelines such as Cobit, as well as financial industry guidelines proposed by the Federal Financial Institutions Examination Council.

Business Focus

Next up was linking security spending and risk management decisions with business goals. To do this, Harland Clarke had to establish some new processes for identifying threats, understanding vulnerabilities and determining which risks it was willing to accept and which it needed to mitigate.

One of these processes is its annual business impact analysis, a three-month-long endeavor conducted by a third-party provider (which Petrie declines to identify) that reviews the company's risk management processes and identifies vulnerabilities or threats to the company's existing controls as they pertain to the goals of the company's five-year operating plan.

For instance, in its contact center, the analysis might look at the controls that ensure call center employees know when calls are being recorded and the controls that protect those recordings from a regulatory perspective and ensure those controls don't negatively impact call answer and handling time. Or it might review the controls surrounding the development of new marketing campaigns. "Because we're getting consumer information, we need to look at how to protect that, and once controls are in place, how that would affect the flow of the marketing campaign, which in turn will determine acceptable risk levels," Petrie says.

Second, Harland Clarke works with Verizon Business (which acquired the company's managed security service provider, Cybertrust, in July 2007) to conduct annual and monthly vulnerability reviews of the entire enterprise, as well as its perimeter. Verizon reviews the controls that Harland Clarke has in place, identifies vulnerabilities, makes recommendations and audits the company's response to those recommendations. For instance, if the security office or executive management team determines that a vulnerability falls within the realm of acceptable risk, Verizon will review that decision and, if it disagrees, will recommend that Harland Clarke revisit the decision. "Risk isn't finite; it isn't a â€œyesâ€ or â€œno,‘" Petrie says. "It depends on what's acceptable to the business to operate."

Risk Matrix

The results of both the business impact analysis and the vulnerability review are then funneled into the development of an annual risk matrix, which combines 20 risk areas, such as malicious code, asset loss and fraud, that are presented to the executive management team. An overall risk score is assigned to each threat, based on whether it's an internal or external threat; its level of potential damage based on a scale of one to 10; and its probability of materializing. From this matrix, the security office determines what actions to take to mitigate risk, which are then approved by the executive management team.

For example, a zero-day worm might be issued a damage score of 7 or 8, Petrie says, and a probability score (assuming controls are in place) of 2 or 3. The risk factor would be determined by multiplying those two numbers and assigning other values, such as what it would cost to shut down the network, and segregate and apply a fix if the worm did penetrate.

"The risk matrix is a tool to help you assign a quantitative number to which you can then decide whether to assign resources and assets to mitigate risk," Petrie says. But because there's only so much capital you can spend, it's up to the executive management team to make the final decision on acceptable risk.

In the end, Petrie says, the company has been able to create an information security program that incorporates repeatable, measurable processes that can be audited and are linked into risk management and the business decision-making process. "Now, security is similar to any other line of business," Petrie says.

In fact, when the different areas of the business develop their annual key performance indicators, security is no different. "We're required to create KPIs and metrics that support those KPIs," Petrie says. Right now, there are

eight KPIs associated with security, supported by 30 metrics that are regularly monitored to ensure the goals are being met. "If we don't meet the metrics within information security, that has an impact on our business goals," Petrie says.

Risk Management in Action

With the security processes and risk matrix in place, Petrie's group has all the tools it needs to make security investment decisions as they arise throughout the year. For instance, it recently discovered through its monthly vulnerability scans and spot checks of its image recordings that one of its VHS-based security recording systems was malfunctioning, affecting 20 to 30 cameras that were attached to it.

One option was to upgrade the entire system to digital; another was to switch out some systems from other locations, as the age of the system made it impossible to find an exact replacement. A controls review indicated that from a cost/benefit standpoint, it made better sense to spend the capital on a replacement digital system, especially because this would enable several locaÂtions in the future to be connected over the Internet to a single operations center. Costs were estimated in the millions of dollars.

The group submitted its results to the executive management team, which agreed that the VHS system posed an unacceptable risk based on the current business model and that replacing it with a digital system would mitigate that risk, both from a quality and a security perspective.

The entire process took about four months, from approaching the executive management team to implementing the first camera replacements. Although going digital represented a 20 percent to 30 percent increase in initial one-time costs over analog VHS, cost savings included physical storage cost reductions and a 20 percent reduction in maintenance costs year over year. It also helped that the camera system was used to monitor the company's quality processes as part of the technical controls portion of the production process, which do have an ROI and an impact on the bottom line.

In a second instance, a Verizon scan revealed vulnerabilities in a production facility: operating systems on its manufacturing line equipment that were not patched adequately. Several months earlier, Harland Clarke had been aware that patches were being offered by the software manufacturer but had made the decision not to implement them because of the possibility of causing a system outage or other negative impact on performance.

Now, however, the scan was reporting that an existing worm had been modified that heightened the risk. This caused the group to revisit its previous decision by running some penetration tests over a 30-day period to determine residual risk and calculate the cost of mitigating the problem. In parallel, it presented the new finding to the executive management team.

"The chances were fairly high that even a low-level worm or virus would shut those systems down," Petrie says. "We determined that it was not an acceptable risk to not apply this patch," especially because it could be applied during maintenance windows rather than bringing systems down.

"The whole process was a complete review of the decision we'd already made several months earlier," Petrie says. "That's why a risk management program is so critical—the threat had changed, so we had to reassess our decision and make a new one based on that."

And that, he says, is indicative of what the security manager's job is all about. "The passage of time is critical," he says. "Risk management is not a stagnant process but a continuous one."