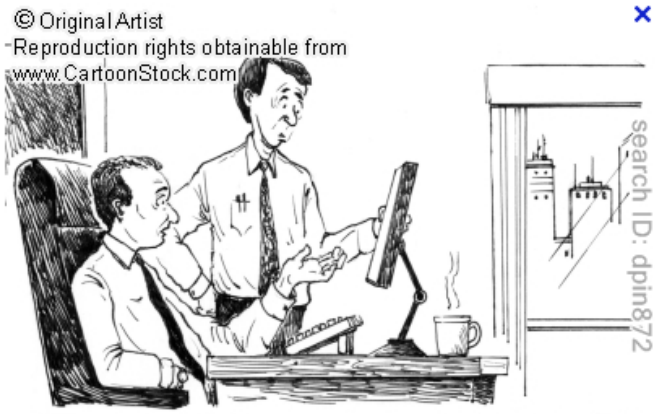
CASE REPORT #5



I don't care if this security software was a bargain; it shouldn't reply with "close enough" when I enter the wrong password.

Name:	Jenet Baribeau, Crissy Rogers
Case Study:	Case 6.2 Security Breach at IKON
Course:	CIS150-01
Date:	12/2/2012

Part 1: Ethical Dilemma

IKON sells specialty clothing. The company embarked on a project to build a B2C (business to consumer) website to supplement their catalog and store fronts where customers could place orders, view the product catalog, and purchase product information. When the website launched, the company was acclaimed for the aesthetics of the website, which were heavily invested in. The primary issue is whether Chester Davis, an IT employee at IKON, should have exposed the associate Vice President of Information Technology for his negligence to ensure the security of the website. The case asks a simple question, what *should* IKON have done? And how do they mitigate the security snafu?

Part 2: Role of IT

The IT Department at IKON should have insisted on continued security services to protect the customer's personal data and the integrity of the website. The IT Department was responsible for the development and launching of the website, as well as the security of the consumer data collected on the website.

Part 3: Stakeholders

1. Chester Davis has the right to develop the security and do his job to the best of his ability without interference.
2. Brian Dobson has the right to enforce his security protocol and IT practices, alternatively, he also has the duty to protect consumer data collected on the website. He ultimately must defend the positions.
3. IKON has the right to run their business as they see fit. They have the duty to provide a secure eCommerce site and protect their customer information regardless of whether it's online, via the phone line or in the store. The data acquired is confidential and used for the corporate purpose as necessary.
4. Customers (of IKON) have the right to expect a standard level of security when shopping on eCommerce websites and feel that their information collected is kept confidential and protected.

Part 4: Analysis of Possible Actions and Outcomes

1. Spoken up during the meeting: Davis needed to explain in the meeting the lengths he went to have security added into the project prior to launch. He doesn't need to sacrifice the VP during the meeting; it appears Davis tried several different avenues to convince his superiors that cyber security was imperative. Clearly, Davis has the experience necessary to recognize threats and manage cyber security; he should have volunteered his services (or been more insistent) to manage the project.
2. Revisit Security after the Initial Creation: Davis should have taken a more proactive approach with the security of IKON's website, especially knowing the extreme vulnerability of the project, after the initial launch of the site. Since there was pressure to complete the project on time and within budget, the security apparently less important than the look and feel of the website, Davis needed to revisit the security issue at a later date. Davis should have managed security patches monthly looking for vulnerabilities regardless of the protest from his superiors.
3. Notify ALL Customers: Since the security breach has already happened. It's ethically mandatory that IKON notify all the customers of this breach so the customer can protect their information. The United States as of yet does not have a federally mandated notification requirements and has been left up to each state for legislation. [1] California is the only one with a state mandated notification but if IKON wants to continue its business, it's in their best interest to satisfy their customers above and beyond anything that could be mandated.
4. Create a Customer Security Policy: There needs to be a policy in place for customer security. A *Terms of Agreement* presented by legal that covers what IKON is responsible for and promises to accomplish to allay the customer. Ultimately, protecting both the customer and IKON by reassuring their customer that they are taking the breach seriously and will continue accordingly.
5. Find a new VP of IT Department: While the VP accomplished his goal, clearly he doesn't value security seriously. He should be replaced. He felt the security breach was a blip when clearly, with a little extra effort and attention this problem, it could have been avoided.

Part 5: Deontological Perspective

From a deontological perspective, IKON should take an action that correlates with their duty to provide a technologically secure marketplace for their customers, who have a right to make secure purchases. Taking this into account, IKON should act according to their *duty* to provide a secure marketplace for eCommerce. Chester Davis should have acted out of his duty as an IKON employee to utilize his expertise in technological security and insisted on protecting the integrity of the company and the website by using adequate protection. Brian Dobson should have recognized the security threat and used ample security allocating the funds from the budget to finance the protection, and worried less about the aesthetics of the website. Dobson should have acted out of his duty as VP of IT, and listed to the IT professional that was informing him about the vulnerability.

Part 6: Teleological Perspective

From a teleological perspective, IKON should have taken the action that did the most good, for the maximum amount of people. IKON pushed for the flashiness of the website sacrificing the security and policies they should have had in place. IKON had a responsibility to protect the shareholders and protect the customer's consumer data with a tiered plan. Even though initially the security "was enough", they should have at a minimum monitored for vulnerabilities. [2] The utilitarian action was to have a Web site that would drive customers to purchase but the consequence was the breach in the security by completely disregarding the pleas of Davis. Had Brian Dobson to listen to his staff member and followed the necessary steps to protect the customers and IKON, this security breach could have been avoided. His consequence should be dismissed.

Part 7: Our Recommendation

IKON did not consider the implications and consequences of setting and forgetting the security for the website. [3] Their focus was on the look and feel versus despite the repeated attempts of Davis to correct the issue. Davis should have persevered after the initial startup and revisit the security issue six months later hopefully with some vulnerability proof. Once the

breach occurred and the discovery meeting called, Davis should have not been the ostrich to avoid causing issues. Since security was his responsibility then he should have owned up to his failure and offered a plan to correct the problems of vulnerabilities. He could have taken some advice on how to create a tiered approach to security with ongoing security checks.

With the "would haves and should haves" out of the way, IKON has a mess to clean up and needs to mitigate the losses and be proactive. The fact that a customer discovered the problem and not an internal test creates a serious doubt of IKON's capabilities online. IKON must notify all their customers with an apology of the breach and a promise to fix the issue going forward with a privacy statement and a dedication to new security procedures. With hopes that with the new procedures in place that their customer base won't leave. This potentially could spread like a virus online with betrayed customers.

The VP needs to leave. Dobson missed the mark and seemingly is flippant regarding the sensitive data breach touting, "it was a glitch". A glitch like that can cost millions from future sales. His attitude alone should be cause for dismissal and had Davis spoken up during the meeting, the other executives would also understand this. The problem wasn't that they didn't consider it. The problem was they chose not to do it and opted for looking pretty instead. With a failure to communicate effectively and forgetting standards especially since they were late to the game to create the Website means there's no excuse for the "glitch". Other B2C sites out there had to be sharing the bugs and pitfalls with some guidance on how to avoid them.

Clearly people value information differently. Had it been email addresses instead of credit card information, would that make the breach less offensive? While the breach isn't good, it can be contained. There are certainly worse hacks that occurred. IKON will recover and live for Cyber Monday. The issue is personnel and critical thinking for this Web site plan.
The security pieces were completely disregarded from the beginning making it a set it and forget it approach. Why build a team if you aren't going to listen to them? Security is now known to be an important aspect to eCommerce and some may say the most critical. IKON needs to clean house and reinvest in the security moving forward.

Works Cited

[1] R. Spinello, Case Studies in Information Technology Ethics, Second Edition ed., Upper Saddle River, NJ: Prentice Hall, 2003, pp. 115-122.

[2] R. Paul and L. Elder, The Miniature Guide to Critical Thinking: Concepts and Tools, Sixth Edition ed., Tomales, CA: Foundation for Critical Thinking, 2009.

[3] National Conference of State Legislature, "Security Breach Notification Laws," 20 Aug 2012. [Online]. [Accessed 29 Nov 2012].

[4] Login Cartoons and Comics, "Cartoons and Comics".