Global Information Assurance Certification Paper

Website Review Leads to Discovery of Non-compliance with the Gramm-Leach-Bliley Act: A Case Study

---

John D. Reilly Jr.

March 15, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment

Version 1.4b

Option # 2

Table of Contents

Abstract 3
Background Information 3
Pre-study Topology 3
New Website Deployed by MYCLIENT 4
Sensitive Data Not Encrypted 5
Website Security Review 5
More Plain Text Communications 8
Researching Legal Issues 9
Vendor Dives for Cover 10
More Legal Research 11
“Situation Report” 12
An Early Opinion 13
Shift in Project Scope 14
Risk Assessment Process and Tools 15
Reworked Assumptions Used 19
Remedial Plans and Priorities 20
A Revisit to Risk Management 22
Risk Tolerance 23
“You’re Wasting Your Breath” 24
Interim and Final Report 24
Lessons Learned 25
Appendix A: Asset Valuation Questionnaire 28
Appendix B: Security Process Model 30
Appendix C: References 31

Abstract

This case-study focus is on a risk assessment I conducted for a small mortgage bank. The project started out as a security review of a website, and quickly mushroomed into a Risk Assessment as part of the Gramm-Leach-Bliley Act of 1999, the FTC Privacy Rule, and the FTC Safeguards Rule. Elements of risk, both qualitative and quantitative were reviewed, a risk modeling tool was used to score the risks faced by the client, reports were prepared, delivered to, and reviewed with the client detailing specific remedial steps identified based on their systems deficiencies. Despite initial ignorance to the GLBA laws, and a resistance to investing in security solutions, some of the corrective measures have been implemented as of this writing. It is estimated that the client will take until the end of 2004 to implement the remaining measures.

Background Information

I was contracted to provide assistance in designing and implementing a project for a company that I will refer to as MYCLIENT, an American mortgage bank. MYCLIENT out-sources all of her IT support and IT management. To protect the identities of those involved, I will define the pseudo names I use in this paper. We will consider her ownership interest as a franchise of the larger organization that I will call "HQ Co." MYCLIENT does repeated business with HQ Co., but has no explicit control over their actions or policies. HQ Co. does have some influence on MYCLIENT, and can create policies for them to follow. While MYCLIENT operates independently for many aspects of her business, significant 'back office' mortgage operations of the two entities are closely related. Third parties involved in the process include the website design company which I will refer to as MARKETING Co. and website hosting company's that I will call WEBHOST-A and WEBHOST-B. All of the employee names and titles used in this paper are fictional.

The satellite office expansion project I was contracted to work on was nearing completion. I had developed a good understanding of MYCLIENT's day-to-day operations and a sense of her appreciation of investment in network security. Unfortunately, our opinions differed significantly when it came to her "less is more" approach to security. For example, it took 6 months of prodding her to invest in a small server with email and a tape backup. Email is a mission critical feature in her business, and bringing it in-house relieved repeated and extended outages with the HQ Co. email server.

Pre-study Topology

The topology of her network included:

- T1 Internet service
- Cisco router with IOS Firewall and Access Lists implemented

- (1) 10/100 Ethernet manageable switch
- (1) Microsoft Small Business Server (SBS) 2003 with tape backup
- a point-to-point (P2P) T1 connection to a remote site
- (2) Cisco Routers with Serial WIC's for the P2P T1
- (1) unmanaged switch at the remote site
- Various shared and networked printers/copiers.
- Clients were either Windows 2000 or Windows XP.
- Applications on the server included a mortgage loan processing program, Veritas Backup Exec, and a Sys-log server.

New Website Deployed by MYCLIENT

During a casual conversation about the current project, MYCLIENT informed me that she paid a graphic design company (MARKETING Co.) for a market campaign to increase the volume of mortgage loan applications for her franchise. That campaign led to the design of a website, and other marketing mediums to draw attention to the site. Based on the lax security attitude I had noticed from MYCLIENT during previous projects, immediate warning signs creaped into my mind and I started to casually probe my client to see if my fears were founded. "What type of website will this be?" I asked. "Will you be taking applications online from customers? Are you going to host the website on your network?"

She explained that the intent of the site was to take online mortgage applications for home buyers and mortgage refinancing, and "the site had been built securely." She further explained that once the application was 'submitted' at the website, it was emailed to HQ Co., which in turn sent her office an email notifying of the new application. She couldn't explain why the HQ Co. had a role in the process. It seemed odd to me that the loan application she was paying to develop was being sent to the HQ Co., and then being forwarded to her office. MYCLIENT explained that the Website design emailed online applications to a dedicated IT person at HQ Co., and then forwarded the lead to her branch. I got the impression the email was encrypted since an IT person at HQ had to receive the email. Maybe that was why HQ Co. was involved, to decrypt the emails.

Since I was already working around MYCLIENTS network, server, and client workstations, I knew no one was using any form of encrypted email, so I started to worry about what I was going to find next. I explained to MYCLIENT that she really needed to be careful when handling online applications containing customer information because the mortgage applications are loaded with plenty of information that would fuel an identity theft. Identity theft is a rapidly growing problem affecting some 7 million Americans in 2003.[1]

[1] Roberts, p. 2.

She didn't seem concerned with my comments. Again, the "less is more" perspective of my client was surfacing here. She also expressed confidence that the MARKETING Co. had pointed out to MYCLIENT the appearance of the "padlock" at the bottom of the application page, indicating the process was securely protected with Secure Sockets Layer (SSL) encryption. "Oh brother", I thought to myself, "she thinks the almighty padlock makes everything OK."

Sensitive Data Not Encrypted

The next day, while onsite at MYCLIENT, I noticed an employee emailing an "electronic" version of a completely verified consumer application to HQ Co. in preparation for a loan to close. I stopped immediately and politely asked her to explain what she was doing. The employee was using their mortgage processing software to send an electronic version of all of the customer's data to the HQ Co. This file was a very detailed review of the financial status of the customer applying for a mortgage. It had everything about the customer in the file. EVERYTHING. I asked her to repeat the process she followed to make sure I understood their office practice. I opened the attached file with Notepad… garbled junk – a good sign of some form of encryption. I then asked how often they send these files. The employee told me they do it for every single loan. I noticed the program had an option for password protection but the employee noted it was *never* used.

That afternoon I called the help desk of the software company used to process mortgage applications. Once I reached a technician, I asked about the email function of their software, and the 'password protect' option. Basically, if the password is not enabled and chosen, any Window based version of their software can read the file. And the level of encryption offered by the software? "40-bit" he answered. Most security conscious applications have adopted 128 bit encryption due to the exponentially greater difficulty in cracking the cipher. In 1997, a commercial machine was built that could crack 40-bit encryption in 5.9 seconds. As such 40-bit encryption is widely regarded as unacceptable for commercial use, and capable of being cracked in real-time.[2] I performed a quick search on E-bay for low cost legal copies of the software. There were copies available for a mere $200.

Website Security Review

It took another 2 weeks for MYCLIENT to finally invite me to review the security of her website, despite several attempts on my part to remind her of the role and importance of information security in her business, and this practice of emailed applications sounded like a security problem. The catalyst occurred during a phone call where I bluntly stated "are you going to have me review this site for you, or did you plan on waiting to get hacked". That got her thinking that maybe she does have a concern with what was

[2] Kocher, p. 5.

deployed. She then explained that it was already up and running and she had received over 100 applications so far. "So much for pre-deployment testing," I thought to myself.

At my request, she immediately called the MARKETING Co. to tell them to answer any questions I might have when I called. She then agreed to my terms and gave me the authority to move forward. At this point, my plan was to ask questions of those involved about the processes followed and the site maintenance and then do some passive testing of the site to get a feel for what I was dealing with. This was before I entertained any type of hands-on work with more aggressive vulnerability testing tools or software.

I went to her website and noticed 2 concerns almost immediately. First, MYCLIENT's online mortgage application was actually a link to the HQ Co. website, and was simply using the existing online application of another website. Second, when I clicked on the link leading back to the HQ Co. online application, there was no information provided on the certificate being offered in setting up the SSL session. I had to fire up a packet sniffer to catch the Certificate Authority (CA) information, and then wade through multiple expired certificates on the CA's website to find the valid certificate. Interestingly, the CA website offered an automated invoice creation tool that allowed me to dump the contact information of a valid IT manager from HQ Co. into a pseudo invoice. That information, which included job title, and office location, could be used to contact employees in a social engineering attempt to learn privileged information at MYCLIENT. Also of note - the CA is located in South Africa.

I then did a few simple tests on each website. First, a reverse DNS on MYCLIENT's website IP address to determine who was hosting the site (WEBHOST-A). Then a lookup on the IP address of HQ Co's website revealed a different hosting company (WEBHOST-B). Using tracert, I found that WEBHOST-A was located on the West coast, and WEBHOST-B was located on the East coast. Again, using the packet sniffer, I reviewed the response from a GET request at WEBHOST-A, which revealed the following, was running:

- Unix based Apache server (v 1.3.27)
- DAV 1.0.3
- mod_gzip 1.3.26
- mod_SSL 2.8.10
- OpenSSL 0.9.6c
- PHP 4.3.4

Using the same packet sniffer on WEBHOST-B, I could see it was running a Microsoft based operating system, and Microsoft IIS Server (v 5.0). Without more explicit authorization from HQ Co., I was reluctant to do more intrusive inquiries.

Already I didn't like what I was seeing on 2 different websites, in 2 different states, with 2 different Operating Systems (OS), particularly with the fact that MYCLIENT's customers were completing loan applications on HQ Co.'s website. "This could get sticky" I thought to myself, since HQ Co. had no contract with me for security consulting. The loan application page prompted for a complete financial history, to include Social

Security Number (SSN), Date of Birth (DOB), employment history, financial assets, and financial liabilities. While I was looking at MYCLIENT's website, I followed along on the online application (HQ Co.) and noticed a disclosure button that was required to be clicked in order to submit the application. I filled out the application with my name and email address, the 2 minimum fields to submit the application, and then had trouble accessing the disclosure that I needed to acknowledge. This was another bad sign that I was being tripped up by their disclosure process. I managed to meet the requirements, read their disclosure about Fair Lending practices, and submitted the application.

Meanwhile, the call by MYCLIENT to the MARKETING Co. must have sent an alarm through them because they were very eager to find out what I wanted to know, and after repeated missed phone calls, they started emailing me. The gist of their opening email had 2 very disturbing phrases. First, the MARKETING Co. said they ***intended*** to implement a secure area of the site with SSL. Second, they said HQ Co. had ***not*** implemented any secure areas for transferring data to their affiliates, and the MARKETING Co. had advised them to do so ASAP. "Oh boy" I thought after reading this, "what is happening with my test online application?"

By now I had a pretty good idea that the MARKETING Co. had not factored much security into the current website, so I thought I'd lob a few questions to the MARKETING Co. to test their understanding of website security, and gauge the level of sophistication and forthcoming I was dealing with. This way I would better understand if secure functionality was not purchased by MYCLIENT, or if it secure functionality was not offered by MARKETING Co.

From my SANS course work and my own experiences, I was familiar with several security issues we needed to discuss, so I drafted and submitted these preliminary questions to MARKETING Co., some of which I already knew the answers.

1. Online applications - how are these transmitted to HQ Co. from the website? I understand they are emailed to the main office. So I'm looking for encryption here; if the emails are encrypted before being sent to the HQ Co. domain, please describe.
1. Login and SSL Sessions - Does the site design track "Session State" with users?
2. Logging - How do you monitor the website for suspicious activity?
3. Backup - Who maintains the backups of the website? What kind of documentation is available on the methods used? Will the responsibility for backups or ownership change in the future?
4. Web Server application - Which specific applications are you using on the website? Do you use a test server (pre-deployment) that we can perform vulnerability testing on?
5. When you say 'plan' [SSL implementation], when will this be implemented? What is currently in place? I understand the site is live and receiving applications.
6. Will you forward to me the written recommendations you have made to HQ Co., so I can evaluate them for MYCLIENT?

More Plain Text Communications

The next morning (Friday), I received and email from a sales person at HQ Co., we'll call him Greg, asking to contact me regarding my recent online application. As I scrolled down Greg's message, I saw it had been forwarded 2 times before Greg actually emailed me. Greg received my contact information via email from another employee, Richard, at HQ Co. the day before. Although I had never heard of either person, it looked like Richard was the person that received the original application that I filled out on the website. Then I nearly fell out of my chair as I scrolled further. The online loan application had been recreated in a simple email format with each field (SSN, DOB, etc.) clearly presented in plain text with the corresponding entry for my answers populated in the blanks. "Oh no", I thought to myself, "this is really bad practice."

Next I looked at the email header options to see what I could learn. Greg's reply address was for the HQ Co., but the source IP address of his email was that of a regional cable ISP as revealed by a Reverse DNS lookup. The IP address was that of the SMTP server of a local cable ISP. A Google search on the SMTP server pulled 86 hits under the newsgroup news.admin.net-abuse.sightings. It is also the exact same named SMTP server from the same cable company. Further down, I could see Greg's IP address, in a completely different range, and a reverse lookup also shows the IP address to be owned by the same cable ISP. It was pretty clear to me that Greg sent the email to me from this cable ISP.

I again did a Smart Whois DNS lookup on HQ Co's domain name, and their MX record, and found that their email server IP address was in a completely different range than the (2) IP addresses contained in the header of the email from Greg. I also believed they were operating their own SMTP server, near their offices based upon a tracert. I concluded that salesperson Greg was working either remotely from his house or Greg operated his own franchise that used the cable ISP for internet access. Neither was of good news to me because it indicated to me that my 'test' loan application, filled with the most private financial information, had traversed the public internet no less than 3 times. They weren't just risking my personal privacy and financial security, they were parading it around oblivious to the problem. Noticeably absent from any of the emails was evidence of prior encryption. An encrypted email message usually leaves a tell tale sign of hashing or keys.

I started thinking about the whole situation in general, and it wasn't pretty. MYCLIENT had received over 100 online applications at that point, and the HQ Co. has scores of other branches, all receiving online loan applications this way. I estimated that they received several thousand loan applications in this manner up to that point. On top of that, every processed application, which contained verified and sensitive financial information, was being emailed back to HQ Co. for every loan. I wrote down what I knew thus far to keep me focused-

- MYCLIENT sends unencrypted email with sensitive information to HQ Co.
- The website links to a 3rd party (HQ Co.) that I have no contract with.

- The website does not offer info on the SSL Certificate.
- The Certificate Authority is located in another country in Africa.
- The website has a cumbersome disclosure related to Fair Lending laws.
- The website sends loan applications via unencrypted email to the HQ Co.
- HQ Co. exchanges the loan emails with branches or employees unencrypted.
- Branches or employees forward the emails to customers unencrypted.

Researching Legal Issues

Now I wanted to see what kinds of liabilities and penalties might be in place for mortgage banking companies that aren't protecting the privacy of customers. I spent a few minutes using Google to research keywords privacy and banking. Numerous hits and links appeared that pointed me to check out specifically the Gramm-Leach-Bliley (GLBA) Act of 1999, among other information.

The GLBA, put out by FTC and other government agencies, governs how financial institutions must treat and protect consumer non-public information. The act defines Non-public Information (NPI) as:

> • any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
> • any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
> • any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).[3]

I spent about 30 minutes surveying the information and its applicability and requirements to my client, and felt confident that MYCLIENT was clearly under the jurisdiction of the law as it relates to financial institutions. I didn't think MYCLIENT was regulated by the 8 or so large federal regulatory bodies like the FDIC or SEC, her company fell under the catch-all umbrella of the FTC jurisdiction. Further analysis of the law described two critical aspects of GLBA - The Privacy Notice, and the Safeguards Rule. MYCLIENT is able to provide a simplified privacy notice because she does not share information with 3rd parties. This relief is provided by the FTC:

> If you don't share NPI with affiliates or nonaffiliated third parties except as permitted under sections 313.14 and 313.15, you can provide a simplified notice that: (1) describes your collection of NPI; (2) states that you only disclose NPI to

[3] FTC: How to Comply, p. 4.

> nonaffiliated third parties "as permitted by law;" and (3) explains how you protect the confidentiality and security of NPI.[4]

I went back to the website and discovered the "privacy notice" as described above was not anything like the disclosures that appeared on MYCLIENTS website, nor were the disclosures that appeared on HQ Co's website. The FTC offers very detailed guidelines on how to craft a consumer privacy notice, and simple suggestions from the FTC, such as the size of the font used "12 point, no less than 10" were not being followed.[5]

The Safeguards Rule is also defined by the GLBA. The rule, which became effective for financial organizations in May, 2003, states a company must

> Develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.[6]

At this point, it was Friday afternoon and I needed to contact MYCLIENT to share what I had learned thus far to alert her to the dangers and liabilities, and to affirm she was prepared to face the rest of the discoveries that I feared. During that conversation I explained the surface level review exposed her to significant liability and was terrible practice of protecting private information. I asked for her legal counsel to weigh in. Her initial response was that their State Department of Banking guidelines were being met, and that's all they had to worry about. I disagreed with her, explaining the reach of the FTC over financial institutions. She was troubled by the news, which was a good sign, so I reengaged her commitment to fully understand her state of security in light of the new information, to which she responded "That's why I hired you." OK!

Since I'm not a legal expert, and I wanted to make everyone involved that I was not trying to portray myself as such, I asked MYCLIENT for her attorney's contact information to make sure a request was made for a legal opinion. I felt it was imperative to have MYCLIENT's attorney weigh in on her obligations to the GLBA. So I called and left a message for her attorney to call back in regards to a question on MYCLIENTS liability, and the GLBA. I was also hoping her counsel would be participating in the creation of the Privacy Notice that I felt was required, and the sooner counsel was brought in, the more aware and helpful they might be. I also emailed several of the FTC documents to the attorney.

Vendor Dives for Cover

Once the attorney was contacted, I turned my attention back to the MARKETING Co. and their response to my 6 questions on the website design and maintenance. Their

[4] FTC: How to Comply, p. 8.
[5] FTC: Get Noticed, p.1.
[6] FTC: Financial Institutions, p. 2.

reply seemed to be crafted with the intent of being a dead end. Absolutely none of my security specific questions were answered, and they tried to shift emphasis away from the relationship between me and MYCLIENT. I also noticed they carbon copied the owner of the MARKETING company in the reply. This was the first time his name appeared in any emails. I discovered his name when I went to their website looking for technical people to contact. Why did they now want his attention in the matter?

Interestingly, while MARKETING Co. was distancing themselves from both me and my specific security questions, they reiterated that MARKETING Co. and HQ Co. were redesigning the HQ Co. website with security in mind. The MARKETING Co. also flat out stated they didn't design HQ Co's current website, or its SSL loan application form. So now I'm getting nothing but bad vibes from the MARKETING Co. and that had me worried. On one hand, I had an obligation to evaluate their work candidly, and on the other hand, I needed their cooperation in the event the website needed changes. I decided to make a call to MARKETING Co. to establish a more productive relationship than we appeared to have thus far.

I telephoned and asked for the contact person at MARKETING Co. Within 30 seconds of taking my call, he told me MYCLIENT's contract with them did not provide for a separate application form with its respective security and SSL features. Hmm, MARKETING Co. already pulled the old contract? He continued to say they would however be happy to work on such a feature as a new contract, and it would be estimated and billed for accordingly. "So much for a more productive relationship" I thought to myself. I made a mental note to get a copy of the old contract to review, but wasn't hopeful I'd find support for MYCLIENT on this issue. 15 minutes after we finished the call, MARKETING Co. sends yet another email recapping the issues, or their position on those issues, and again stating a secure application wasn't part of the original deal. "Wonderful" I thought to myself. MARKETING Co. wants some money before they'll consider any changes to the site. To top it off, MYCLIENT did not have a copy of a proposal or a contract – just a paid invoice.

By now, the people I had come into contact with in regards to the GLBA were rather blasé or ignorant to its requirements. During my previous projects with MYCLIENT, I got a pretty good 'feel' she did not have much interest in investing in security technologies other than a basic firewall, a basic server, and good email anti-virus system. Perhaps I was blessed to get that far. Based on the quantity of GLBA compliance material I was finding and the language contained within, I was even more concerned now with her lack of interest in compliance, and MARKETING Co's current website design, regardless of who was ultimately going to pay for changes.

More Legal Research

So I turned to the State Department of Banking. I knew that MYCLIENT was regulated by the state, and wanted to see if the GLBA was on the state examiners 'radar' - if the GLBA was something they took seriously in their audits. So I made an anonymous call,

and waited to get an examiner on the line. This call was a total dead end – the State was only interested in issues that could be found directly within the "file" of the loan application. In other words, they were looking at lending fees, fair credit issues, etc., none of which were specifically addressed by GLBA Privacy or Safeguard rules.

Next I made an anonymous call to the FDIC, one of the 8 governing bodies (FDIC, SEC, etc.) referenced in the GLBA that would possibly enforce MYCLIENT. Of those 8, the FDIC seemed to have best chance of having interest in MYCLIENT because as a mortgage bank, MYCLIENT collects escrow deposit payments. However the FDIC does not audit mortgage banks per se. Determined to not let the opportunity pass, I asked the examiner how they would react based upon an institution they did audit. I described a generic situation, without naming companies or employees, and the practice of emailing unencrypted consumer loan applications, to which the FDIC examiner replied "we would be very upset with that discovery". The issue struck a nerve with the examiner and changed the tone of the call. The examiner added that since MYCLIENT was not regularly audited by one of the 8 federal governing bodies, their compliance risk would come in either the form of a consumer complaint, or an investigation started by the FTC. I wasn't able to find a quick phone number to question an FTC examiner, but I was pretty confident that MYCLIENT was firmly in their lap for enforcement, so I put that call off for a while.

I wasn't really getting the traction I felt I needed in regards to the 'bite' or applicability of the GLBA and MYCLIENT, and I knew at some point, more interaction was going to be needed with HQ Co. I started the process of tracking down the appropriate IT person or department at HQ Co. After some legwork, and a quick call to MYCLIENT, I confirmed and verified the top IT person at HQ Co., we'll call him SECURITYGUY, and I emailed and called him to introduce myself. Since it was late in the day, I did not expect an answer until the next morning. I hoped this would be a productive avenue.

Two other issues were lingering in my mind at this point. First, why hadn't I heard back from MYCLIENT's attorney? Second, I was still bothered about the response I received from the design company, and didn't want them thinking I was going away, so I emailed MARKETING company again and asked them to define their idea of "redesigning with security in mind". Since they say they have a plan, it must be in writing, or somewhat familiar to them, and could then be put in writing for me to review. I expected another bland response but felt I had to determine their capabilities in this area.

"Situation Report"

It was nearing 6:45PM when MYCLIENT called back. I shared the information I learned from the State Department of Banking and FDIC. She didn't seem fazed. I got the sense that if the Department of Banking didn't bring up compliance issues like GLBA then it wasn't a concern of MYCLIENT. (I went on to explain that, in my opinion, based upon the readings and conversations I had that day, her company is clearly under the realm of the Federal Trade Commission (FTC); there is clearly an expectation of compliance;

clearly a liability for them in multiple areas). Plus I said “it’s just plain wrong and a bad business practice to be sending customers personal information out across the Internet in plain text.” With less confidence in her voice, she then stated weakly that her current Department of Banking required Disclosures are adequate in regards to the GLBA Privacy Notice. I was ready for this line of reasoning, and pointed out significant differences between what her disclosures contained, and what was asked for from the FTC.

Now MYCLIENT is the successful owner of her business for a reason, and the problem solving gears started turning in her mind. MYCLIENT wants to know what is required to bring her site into compliance, and adds “We can change the Privacy Notice easily can’t we?” I quickly recalled the point my GIAC Instructor Eric Cole raised while addressing Basic Security policies. He pointed out the danger of adopting a policy that isn’t enforced, or enforced inconsistently might be more dangerous to an organization than having no policy at all. In this case, if MYCLIENT posted a Privacy Policy that was false or inaccurate, she could be guilty of fraud. I also added that it was imperative we get feedback from her attorney, because I’m not a legal expert.

I continue to describe some of the requirements of GLBA like policies, assessments, testing, remediation, etc. and she had no idea what they meant, the cost involved, nor the time to implement them. While uncertain of the quantity of those things myself at this point, I did know it won’t be cheap or quick fixes. However, I added “it’s not a problem you can solve in isolation. Encrypted email does you no good if the recipients can’t open it.” Since she doesn’t operate in a vacuum, and every loan application gets emailed to HQ Co., she starts to see the scope of the problem, and the role of their HQ Co. She again asks “how long will it take to become compliant?” I surmised, “in a best case scenario, which is unlikely, it might take a month IF all of the companies involved cooperated, ‘bought-in’ to the process, purchased and or implemented corrective actions, trained staff and management, and had the same enthusiasm for the plan.” As I finished that last sentence, we both new this would be a much longer project than 1 month. Thinking towards the first step, MYCLIENT said, “call the Director of IT at HQ Co.” I said “I already did”.

An Early Opinion

That evening, I set 2 tasks for myself. I wanted to further my knowledge of the MYCLIENT’s legal requirements, and I felt an early written report to MYCLIENT was in order. While I had explained the dangers of the current practices, I don’t think the seriousness of the issue was sinking in. Putting my concerns and opinions in writing, with strong language and before the project was completed would hopefully set a serious tone and perspective. It also would provide “CYA” value.

I used Google to specifically query on Sans.org with keywords FTC and Privacy. I found some excellent resources, several of which were close to MYCLIENTS situation. First, I read the paper by Angela Noomis – “Bank of Newport and System Security –

Minimizing your Liability" and the paper by Kevin Bong, "Conducting an Electronic Information Risk Assessment for Gramm-Leach-Bliley Act Compliance. After I read their papers I felt more prepared to provide an early opinion to MYCLIENT.

Below is the body of the email I used to repeat concerns on the serious risks to privacy that I identified up to that point:

- Your web site and your current business practices are not in compliance with the Gramm-Leach-Bliley Act (GLBA), the Privacy Rule, nor the Safeguards Rule.
- Your web design company, MARKETING Co., has not yet demonstrated a grasp on designing or maintaining a secure website.
- I have emailed and telephoned your attorney to legally advise you on how applicable GLBA is to your business.
- You and or your HQ Co. have an obligation to ensure people you do business with are in compliance (i.e. Credit Reporting/Appraisal/Settlement) with GLBA.
- You should immediately stop accepting online consumer loan applications through your website until the items A - E below are addressed.
- Address the specific requirements of the Safeguards Rule from the Federal Trade Commission to include:
  - A) Complete a written risk assessment.
  - B) Develop written security policies.
  - C) Reduce identified security risks with commonly accepted measures.
  - D) Develop an acceptable Privacy Notice for GLBA based upon B & C.
  - E) Train your staff and managers on the importance and practice of protecting information.

Turning back to my research, Angela Noomis introduced the Open Web Application Security Project (OWASP) and the Top 10 Vulnerabilities of Web applications.[7] These issues would contribute to a growing list of questions and concerns for future discussions with the MARKETING Co. Kevin Bong's paper offered an excellent discourse on the Risk Assessment process he went through at his financial organization, and he developed a tool to automate a significant portion of the process and freely offered it on his website.[8] I also went back to the FTC Website and downloaded all of their GLBA documents.

Shift in Project Scope

The initial task of reviewing MYCLIENT's website for security had taken a major turn in scope. What had started out as a narrowly defined project to evaluate functionality and security of a website had mushroomed into a study of her entire organization. However, the chain-of-events that led to the shift in scope were logical, since the Website review triggered the discovery of the GLBA privacy and safeguards requirements. And those

[7] Loomis, p. 7.
[8] Bong, p. 4.

requirements are detailed, touching every level of the business. I added to my list of concerns started earlier the 5 explicit items as specified by the FTC Safeguards rule:

> 1. Designate one or more employees to coordinate the safeguards;
> 2. Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
> 3. Design and implement a safeguards program, and regularly monitor and test it;
> 4. Select appropriate service providers and contract with them to implement safeguards;
> 5. Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.[9]

Although MYCLIENT could immediately start tackling individual fixes for glaring problems, it was clear to me that at some point the Risk Assessment had to be completed, and it might turn up other problems that are more serious, and or could be addressed at the same time. I also felt that I had a solid grasp of MYCLIENT's systems from previous projects, interviews, and correspondence. Since the GLBA specified legal requirements, and MYCLIENT expressed a desire to become complaint, I felt we were at the 3rd step of the Risk Management Process as outline during the course work of SANS Security Essentials and the CISSP 10 Domains. Step 3 of the SANS process is to perform a detailed study of the risks and vulnerabilities, or recognize best practices for this particular industry.[10] It was time for a Risk Assessment.

Risk Assessment Process and Tools

For the actual Risk Assessment, I chose to use the model developed by Kevin Bong. It was produced as a practical paper reviewed by security professionals and the paper is posted on the SANS website The model has an affiliation with SANS, it is easy to use, it's free, and I had confidence that it's scoring, assumption flexibility, and reporting features would help MYCLIENT meet the requirements of a GLBA Risk Assessment. To further support my decision, the Federal Financial Institutions Examinations Council states in its IT Examination Handbook that an adequate Risk Assessment produces "a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products"[11]

Turning back to Bong's assessment model, I followed through steps 1 through 4 to classify the type of data used by MYCLIENT, determine the level of importance the information or system has to the business, inventory the systems in use by MYCLIENT, and then classified the systems level of importance[12]. Since "Step 4: Determine Initial

[9] FTC: Financial Institutions, p. 2.
[10] SANS: Risk Management and Auditing, p. 830.
[11] FFIEC: Audit, p.15
[12] Bong, p. 4.

Risk" retained the settings used for Bong's financial institution, and was in response to his own GLBA requirements, I left the default classes of risk unchanged. To illustrate the applicability of the default settings to MYCLIENT, I considered Bongs rational behind the highest risk category:

> Being a financial services company, reputation and compliance are among our highest priorities. We determined the attributes of our initial risk categories based on this:
>
> **Highest Initial Risk**
> Failure or compromise of this technology or vendor
> - Can cause disclosure of private customer information
> - Can cause us not to stay in compliance
> - Can cause significant impact on the reputation of the company[13]

Once steps 1 through 4 were completed, I could prepare an initial risk report as depicted in **Figure 1**. The Categories to the right hand side of the report denote the types of information stored or transmitted in a technology. For example, CAT1 [short for category 1] means the system has NPI information, and is treated with Highest Initial Risk status. CAT7 means the system has mission critical features, and CAT8 means the system is critical to providing customer service. CAT7 and CAT8 in Bong's model are treated with High Initial Risk factors due to importance to the business. MYCLIENT communicated similar valuations on these categories, so I left the default classifications in place.

rptSystemsCategoriesTiers

System	Group	Tech.	Vendor	Tier	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Cat 6	Cat 7	Cat 8
Internet T-1 and Router	Internet Connections	X	X	Highest Initial Risk	X		X	X	X	X	X	X
MYCLIENT.com Website	Web Servers	X	X	Highest Initial Risk	X	X	X		X	X	X	X
Network Switches	Network Infrastructure Device	X		Highest Initial Risk	X	X	X	X	X	X	X	X
P2P T1 and Routers	Network Infrastructure Device	X	X	Highest Initial Risk	X	X	X	X	X	X	X	X
PC's with: email, app's, files.	PC and Desktops	X	X	Highest Initial Risk	X	X	X	X	X	X	X	X
Printers / fax machines / output tray	Printers, faxes, copiers	X		Highest Initial Risk	X	X	X		X	X	X	X
SBS 2003 / Exchange Server	Windows NT & 2K File Server	X		Highest Initial Risk	X	X	X	X	X	X	X	X
Telecommuter PC's	PC and Desktops	X		High Initial Risk		X	X		X	X		X

Figure 1 – Initial Risk Report

The next three steps of Bong's Risk Assessment model were relatively straightforward, and did not require much judgment on appropriateness to MYCLIENT. Step 5 consolidates similar technologies to reduce redundancies in reporting and assessment, which will lighten the work of the whole assessment. Being a small business, MYCLIENT did not have that many overlapping technologies. Step 6 called for

[13] Bong, p. 7.

associating the vulnerabilities and threats that were applicable to MYCLIENT technology groups. The prepared list was significant in terms of depth and breadth of threats, and I did not feel additional research for threat categories was warranted at this point. Step 7 lists controls that could be implemented that would mitigate the threats to MYCLIENT from step 6 and again I felt were adequate for the assessment of this client.[14]

Steps 8 through 10 I felt were the crucial decision making steps on the part of the risk assessor. Step 8 added granularities to the controls listed in Step 7 and separated them into preventative, detective, corrective, or directive measures. I thought this to be a critical element of Bong's model as it clearly worked to apply the concept of Defense in Depth.[15] The mindset behind Defense in Depth is that if one type of protection in the network fails, there are additional systems and or processes in place behind it to fill the void. Furthermore, we need a method to detect 1 or all of the layered failures and a process to evaluate what went wrong, to make adjustments for preventing similar failures in the future.[16] Interestingly, Bong notes that Directive controls, otherwise known as policies, relate to measures of influencing behaviors, and since we can't always guarantee human behavior, they are not used in his model of calculating risk.[17] Perhaps some would argue the this decision, but I agree with his cautious outlook, and his general decision to leave Directive controls out of the risk calculations that are applied later on.

Step 9 looks to determine what the adequate levels of control for each given category of Initial Risk we identified in Step 4. Again, the approach of defense in Depth, layers as SANS describes, is clearly practiced in this step, and I used his default definitions. For example, the default settings for a "Strong" definition of internal controls is:

> In the abstract, [strong] assumes layered security, a reliable means for detecting and alerting to a compromise or failure, a means for tracking events and changes or researching past events, and a process to respond, recover, and prevent future occurrences.
> For a given vulnerability, there exists
> - at least two layers of preventative controls which directly prevent exploit of this vulnerability
> - at least one detective control which will reliably detect an exploit of this vulnerability in a very short time
> - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences[18]

Step 10 of Bong's model defines our accepted level of residual risk. This is another step that might be adjusted from the default definitions, but since those defaults are

[14] Bong, pp. 5-7
[15] Bong, pp. 12-16
[16] SANS: Defense in Depth, p. 293.
[17] Bong, p. 13
[18] Bong, p. 14

likely used as baselines for other financial institutions, I kept the existing definitions. Essentially, if any aspect of a systems control encounters a weak classification, then the entire control set of that technology or application is downgraded to the weakest link.[19]

Step 11 through 13 of the model relate to reporting and follow up. Since one aspect of the GLBA is a written risk assessment, this was an excellent time to print all of the reports and organize them into a binder to jump start MYCLIENT's compliance obligations. That was the good news. However, the bad news is shown below in the printout from Bong's model in **Figure 2**.

Well, MYCLIENT was certainly not going to be happy with this news. But before I presented her with this, I wanted to have recommended corrections at least identified and hopefully with costs and estimated time frames. This would prove tricky because there is an inter-dependency with HQ Co. However, when I went through the detailed reports in Bong's assessment model for MYCLIENT, and evaluated what was needed to move her to levels of medium or low residual risks, I believed that the requirements

Systems Summary

systemName	TierName	WorstControlAdequacy	resultingResidualRisk
Internet T-1 and Router	Highest Initial Risk	3-Weak	High
MYCLIENT.com Website	Highest Initial Risk	3-Weak	High
Network Switches	Highest Initial Risk	3-Weak	High
P2P T1 and Routers	Highest Initial Risk	3-Weak	High
PC's with: email, app's, files.	Highest Initial Risk	3-Weak	High
Printers / fax machines / output	Highest Initial Risk	3-Weak	High
SBS 2003 / Exchange Server	Highest Initial Risk	3-Weak	High
Telecommuter PC's	High Initial Risk	3-Weak	High

Figure 2 – Residual Risk for MYCLIENT after existing controls evaluated.

were out of line, and probably more rigorous than necessary for GLBA compliance. For example, MYCLIENT has deployed UPS devices for every PC, the server, and the networking equipment in data closets. For a small business, that's a significant level of protection from temporary power outages that could cause data loss. The default decisions in the model would have her install a power generator to reduce her risk to moderate, and I felt that was overkill for MYCLIENT.

[19] Bong, p. 16

Reworked Assumptions Used

So I went back through the entire model again and changed assumptions, classifications, etc., to reflect what I felt were reasonable for a business of this size. The Systems Summary report yielded the same results, because each technology in use still had an element of weak control. However, the quantity and type of weak controls were now more reasonable to correct in my mind. MYCLIENT might still have objections about cost and impact on her business, but at least an individual vulnerability and its corresponding control wouldn't have a disproportionate cost to implement. Again, the best example here is the risk posed by Power Failure. If I had left the default decisions in the Bong's model unchanged, reducing the risk of Power Failure would require installing a back up generator, which can be an expensive investment for a small business.

The depth of vulnerabilities and controls established in Bong's model makes the tool immediately useful. I believe using Bong's established classes and descriptions is acceptable for an organization engaging their first Risk Assessment. I'd even consider it a base-line for a small organization. Once a company addresses all of the categories in the Bong model, they could begin to work on more granular issues.

Now that we had a significantly clearer understanding of the risks facing MYCLIENT, I sorted through the provided controls and made choices in technologies and policies that I believed would be reasonable to accomplish in light of the criteria established through conversations with MYCLIENT:

- Seriousness of risk to NPI (i.e. Internet exposure).
- Cost to implement, maintain, and train users (often called Total Cost of Ownership).
- Could be completed in 6-9 months.

My goal in using these criteria was to restore confidentiality, and integrity to MYCLIENT's electronic communication, and increase the likelihood of availability. I believed this to be a reasonable accomplishment time frame of securing and implementing the technology and or policy controls. Some of the controls would have to be purchased, configured, tested, and refined over a period of months.

Applying the above criteria to the existing classes of control measures produced a list of measures that could be implemented. However, we wouldn't want to implement all possible remedies for every vulnerability. Rather, we wanted to ensure a solid "defense-in-depth" within a reasonable scope and cost for this business. So I ran "what-if" scenarios through the model to see if particular measures would be sufficient to bring MYCLIENT up to the level of Moderate Risk on her technologies and systems.[20] For each listed vulnerability I would add controls into the model, or take redundant control classes away, until I could achieve a Moderate residual risk in the categories shown in **Figure 3**. While the model allows this type of usage, it is not strongly suited for this

[20] Bong, p. 20.

purpose in the provided format, and I actually saved the original report as a different name, to preserve the information.

Two technologies in use, MYCLIENT website and Fax Machine output pose unique challenges and their resolution will be treated separately. First, the MYCLIENT website has several parties involved in its design, maintenance and hosting. Added to the complexity is the direct linkage to the HQ Co. site, and an additional variable that the MARKTING Co. might be replaced. The output trays of printers and faxes occasionally contain documents that have NPI information. Often, these documents are faxed in "after hours". Both of these issues will be addressed separately from the "Remedial Plan".

Remedial Plans and Priorities

The actual task of bringing MYCLIENT's network into our targeted "moderate" residual risk state was quite large. The FFIEC Information Security Booklet – December 2002 guidance outlines three phases of risk assessment: "information gathering, analysis and prioritizing." [21] Prioritizing became the next tricky part. I had to make recommendations based on the risks to the business and risks to GLBA protected information, while keeping in perspective the resources of MYCLIENT, and the time required to correct

Systems Summary

systemName	TierName	WorstControlAdequacy	resultingResidualRisk
Internet T-1 and Router	Highest Initial Risk	2-Adequate	Moderate
MYCLIENT.com Website	Highest Initial Risk	3-Weak	High
Network Switches	Highest Initial Risk	2-Adequate	Moderate
P2P T1	Highest Initial Risk	2-Adequate	Moderate
PC's with: email, app's, files.	Highest Initial Risk	2-Adequate	Moderate
Printers / fax machines / output	Highest Initial Risk	3-Weak	High
SBS 2003 / Exchange Server	Highest Initial Risk	2-Adequate	Moderate
Telecommuter PC's	High Initial Risk	2-Adequate	Moderate
WAN Routers	Highest Initial Risk	2-Adequate	Moderate

Figure 3 – Accepted results of "What-If" scenarios.

problems. On top of that, 2 critical elements had extensive relationships with 3rd parties, adding significant layers of complexity to the corrective process. I prioritized

[21] FFIEC: Information Security, p.8

MYCLIENT's concerns based upon the dollar cost of the remedy, ease of implementation, and potential gain in the level of security.

I separated the corrective steps into 3 Phases. Phase 1, was to include activating or configuring features already present in MYCLIENT's network, and could be done so in a relatively quick manner, at relatively little cost, and with minimal end user training. Phase 2 included more intricate projects that required the purchase of hardware and or software, and could be implemented over a period of weeks, and then refined. More extensive training would be required in this phase. Phase 3 was for the bigger ticket items that required significant resources and or time to implement, and would be pursued over a period of months with MYCLIENT, and possibly involved 3rd party contract negotiations.

Phase 1 – The following tasks were chosen for immediate implementation.

- Automatic screen savers with password access.
- Strong passwords and lock-out policy.
- Designate an employee to handle security and privacy issues.
- Utilize basic encryption of customer applications before being emailed.
- Logfile monitoring.
- Authentication required on VPN (certificate).
- Authentication event logging.
- Periodic forced password changes.
- Physical access controls.
- Managed switch report and authentication logging.
- Backup job scope revision and alert mechanism.
- Simple tape backup rotation plan.
- Egress ACL filter on Internet router.
- Securing of on-site Fire box.

Phase 2 – These tasks would take longer to implement and or develop.

- UPS with client alerts and automatic shutdown.
- Redundant Internet connection (DSL).
- Incident response policy (with passwords in sealed envelope in firebox).
- Internet use policy.
- Wireless access point policy (WAP).
- Terminated employee process and policy.
- Account and user rights management.
- Desktop antivirus consolidated management.
- Desktop software installation policy.
- Backup monitoring systems.
- Backup policies and procedures.
- Off-site storage.
- User training.
- Change management process.
- Testing and migration plan for software upgrades and installs.

- Designate a security person and define role and responsibilities.
- Confidentiality policy for vendors and contractors.

Phase 3 – These tasks require additional resources and or time and will take weeks if not months to fully implement, refine, and utilize.

- Network-based Intrusion detection system (NIDS)
- Network management system (i.e. HP Open View)
- Service pack/security patch tracking system. (i.e. Hfnetchk)
- Fully encrypted email with HQ Co. and 3rd party relationships.
- WAN provider agreements.
- Vulnerability Testing (i.e. Nessus)

Special – the next 2 categories require significant business process and or vendor review and modification.

- Website concerns-
  - Encryption
  - Privacy Notice
  - Vulnerability testing (OS and Application)
  - Change management
  - Backup and monitoring

- Fax output – Technology or process to limit inbound faxes from sitting in output tray, specifically after-hours (i.e. fax server).

A Revisit to Risk Management

Now that I had an excellent picture of MYCLIENT's network, the risks to her business, and the risks to GLBA protected information of her customers, I felt confident in talking about the corrective steps to be taken in each of the Phases I assigned them. Convincing MYCLIENT to pay for them was going to be another matter. Despite the legal requirements, and the real threats to MYCLIENT's network, she might not perceive them to be credible threats, or she might just decide to "ride-out" the risk until a serious incident occurs. The idiom "You can lead the horse to water but you can't make it drink" aptly described the chance MYCLIENT would do nothing. This is known as risk acceptance, or "willingness to live with the consequence in the event that risk is exploited."[22]

It then dawned on me that MYCLIENT had another significant, unidentified risk at that point. The risk of compliance action from the FTC in the form of a cease-and-desist order and civil litigation. Since the FTC doesn't actively look for Privacy and Safeguard violations, I estimated there could be at least 3 ways MYCLIENT could "appear" on the FTC Radar.

[22] SANS: Risk Management and Auditing, p. 834

1. A consumer could file a complaint. Given the frequency in which the consumer applications were generated and e-mailed to various employees, and then ultimately back to the consumer, I felt there was a significant chance of a wise consumer noticing the problem, and filing a complaint.
2. A disgruntled employee. People do crazy things. Could a terminated employee or an employee facing disciplinary action make a complaint? Very possible.
3. A competitor. Could a competitor try to make life difficult by snooping over MYCLIENT's website, submitting an application, and watching with glee over the weakness in their systems, making notes, and tipping off the FTC? Very possible.

I wasn't sure how to present this risk. It didn't seem to fit into the model I had used to that point, so I would have to consider reporting of this significant risk.

Risk Tolerance

Up to this point, the entire process I used had been a Qualitative risk assessment. In Qualitative risk assessments, "the results are typically categorized as low, medium, or high risk events"[23] We weren't talking in monetary costs yet. Since the corrective actions, my 3 phase plan, were going to require monetary investment, I knew I needed to have hard dollar risk estimates available for her consideration.

Essentially, I was gearing up for an Interim Report to MYCLIENT. The SANS Institute defines an Interim Report: "This report should include a project summary . . . the report should also contain an asset identification and valuation report. This information is critical, since management will then have a better understanding of . . . the valuable assets, and help better justify the cost of countermeasures to protect them."[24]

While I could have produced my own estimates of the assets identified, I knew from experience that having the customer associate or derive their own values is immensely more useful. It eliminates objections that arise during decision making like "We don't agree with how you value that asset". Customer derived values are also more realistic, since they should know their business better than I do.

I prepared a list of assets and questions pertaining to those assets to prod MYCLIENT into using accurate estimates. I also explained why I was asking for the information, and the value of completing the exercise in her overall decision making process. An example of my asset valuation questionnaire is attached in Appendix A:

[23] SANS: Risk Management and Auditing, p. 841
[24] SANS: Risk Management and Auditing, p. 864

"You're Wasting Your Breath"

I followed up with MYCLIENT regarding the questionnaire I provided and was informed she had no intention of answering the questions. She was more interested in selling, and perfectly resigned to the FUD (Fear, Uncertainty, and Doubt)factor in deciding on the security measures I was recommending. "So much for informed decision making" I thought to myself, "the horse isn't thirsty." During this conversation, I also learned that she intended to keep using the website in its current form, but would seek my help in the site expansion plans that were underway.

Interim and Final Report

I compiled my Bong Risk Assessment Summary Reports, my "What-If" Accepted Residual Risk Report, my early professional opinion, the 3 phased remedial plan, the blank questionnaire, and a cover letter. Then I created a section that contained the recommended corrective steps to be followed, and organized it into the 3 phases identified earlier.

For Phase 1, I prepared a Cost Estimate for remedial steps to take. This was the easiest Phase to estimate, and the total was reasonable to both me and MYCLIENT. She agreed to implement each of the items in this phase, although not exactly the way I recommended they be implemented. Several of the items she initiated immediately, and with her own twist on the remedy. For example, she scheduled a locksmith to install a dead bolt lock on the server room with (4) 'Do Not Copy' keys, and moved their small Firebox/safe into the room. Both were significant steps forward in securing valuable assets.

Other examples:

- Password protected screen savers, strong passwords, and system lock-outs after 5 failed attempts were all implemented with little fuss.
- The basic, 40-bit, encryption provided in the processing program was utilized with a single password that was shared via a telephone call to the HQ Co. recipient.
- Backup tape rotation with daily incremental backups, weekly full backups, and daily offsite removal of previous night's backup with a trusted employee were implemented. Significant training was provided for the 2 backup operators to monitor backup reports and tape rotation and cleaning procedures.

Phase 2 also included a Cost Estimate, but this estimate was less detailed and provided only a range of potential costs due to the complex variables, and MYCLIENT's level of participation, particularly for policy development. She balked when I described the participation I needed from her in developing policies that the company would follow and enforce. I stressed that making a policy that was enforced inconsistently or not at all was a waste of her time and money, possibly more risky for her business than no policy

at all. MYCLIENT wanted to delay a decision on most of these items steps for several weeks.

Phase 3 didn't include Cost Estimates for any remedies. The complex issues in Phase 3 required additional in-depth analysis work, testing, deployment time, and revising to be successful. Without a commitment to those projects, or an open contract for completion, I was not going to invest my resources in preparing a detailed estimate, or a solution, particularly with detailed statements of work. However, MYCLIENT did initiate the process to address the Website problems, and scheduled joint meetings with me, MYCLIENT, and MARKETING Co., to work on a solution that satisfied all of our needs. Also underway were separate discussions with myself and the HQ Co. regarding their website, NPI in email, risk assessment, and other security measures.

The Final Report had all of the available printouts from the Bong Risk Assessment tool, including the detailed system and "what-if" reports, notes of conversations, emails with MARKETING Co. and HQ Co., my recommendations, and suggestions for corrective actions. To help illustrate a new perspective on security for MYCLIENT, I created an analogy diagram to illustrate the relationship between risk assessment, policy design, and vulnerability testing, with interlocking gears that are rotating. Sometimes a visual relationship of concepts will make a stronger point – the adage a "picture is worth a thousand words" idea. The example of the model I used is in Appendix B. In the final report, I also noted which measures had been implemented thus far, and summarized again the remaining issues. These were all organized into a binder and clearly labeled and tabbed for easy reference.

Lessons Learned

I found it important to keeping an open mind in regards to any type of security reviews being conducted, and an inquisitive mind in general when working around a network. Some of my best findings during the process occurred by just observing users going about their everyday tasks.

While I am hopeful that all of the remedies and policies will be adopted and maintained with some frequency and urgency by MYCLIENT, the degree and rate of acceptance is not the level I would have hoped for. I'd estimate that the client has completed 15% of the remedial steps, and has a clear interest in engaging approximately 35% more of the 3 phased approach. However, the remaining 50% have significant safeguards like the policy development, an IDS system, end-to-end email encryption, and revamping of the website. Despite conversation, articles, and training, it appears that the benefit of those projects still seems intangible to MYCLIENT. Although we satisfied a big requirement of GLBA by completing the written risk assessment, more work is to be done at MYCLIENT to come full circle with the spirit of the rules.

A couple of warning signs I'll note for future work include A) an unwillingness by the customer to participate in valuing identified assets as part of risk management may be a

significant indicator of unwillingness to invest in security to mitigate existing levels of risk. B) Lethargy from a clients counsel might also reflect a risk tolerant or risk ignorant environment for the engagement. For example, MYCLIENT's attorney finally responded to my request but not directly to me. He called MYCLIENT and told her he could "care less about it". This same attorney performs real estate settlements and financial planning services.

Even though my SANS instructors warned me not to be surprised by managements decision to accept current levels of risk, in this case information systems and consumer NPI, I was still surprised! I've been involved in IT for 5 years, and I've seen indifference before but it's not a welcome response in any engagement.

The interaction with MARKETING Co. reinforced persistent, direct questions are an important part of the process. Just because a website is graphically appealing and organized, doesn't mean it's secure, or that web designers by default take security into account when designing web pages. By not accepting 'pat' answers from employees, management or contractors, I was able to push into the core of their understanding, and truly evaluate the state of affairs. By "peeling back the layers of the onion" I was able to probe further with each round of information exchange to get the hard evidence that would refute or prove their statements. These statements were critical in understanding the systems and process in use in MYCLIENT's network and her business.

As it turns out, the graphic design company is just that. I learned during discussions with MARKETING Co. that any type of security "programming" required on their part is sub-contracted out to a PHP specialist, "who knows all about security."

I'm rather disappointed with the publicity around the GLBA, the FTC Privacy Rule and the Safeguards Rule. It's unfortunate that the extent the FTC Safeguards Rule isn't widely known or regarded by the Small to Medium size Businesses (SMB) it covers. General awareness of GLBA needs to be raised. A significant portion of this act is squarely aimed at this market space, but seems to have little traction, let alone awareness.

For privacy and protection efforts to be raised, this has to be improved. I believe this can be achieved when the FTC gets more visibility on enforcement issues and cases, the dollar amounts of penalties become public and significant. Then, there will be more 'bite' in the risk of FTC enforcement actions. It seems that this risk needs to feel 'real' to the SMB market to consider it more seriously.

In addition, future Risk Assessments need to factor FTC enforcement action, assuming the client chooses to not mitigate existing risks. This "Compliance Risk" needs to be addressed with a metric and calculated for use in further risk management discussions. I will look to build a treatment for this in my future uses of Kevin Bong's model. While distasteful, security professionals will have to evaluate this risk.

A pleasant surprise in the project came from the calls and conversations with state and federal examiners. I figured it was a long shot and I'd reach voicemail and never get calls back. However, most of the calls were fruitful. I plan to utilize those lines of communication in future projects.

I believe the key for me to help my client become compliant is to convince both her and HQ Co. to take the lead and dictate policy, shoulder the burden of choosing technologies, and force compliance down the "ladder". Persistence exposure and reminding MYCLIENT has had success in the past on issues. I plan to "keep the pressure up" on completing all the phases of her corrective action plan.

Since HQ Co. was actually more responsive, I believe there will be downward pressure on MYCLIENT to complete her plan as well. With more branches at stake, more in-house expertise (IT staff, Compliance attorney, etc.), the HQ Co. will hopefully go through a similar process and see it through to completion. While HQ Co. still didn't know about GLBA, they did react much quicker and more strongly to the concerns once informed.

HQ Co. has technical skill and aptitude to participate in the study, even in-house legal counsel. However, all seemed "over-worked", unsure how to start fixing the situation, and generally relieved to have a 3rd party worry about risk and assessment for them. I'm positioned to fill that role, and hope to have all parties on board, "kicking and screaming", if necessary.

Last, some advice to consumers: be sure to factor safeguards compliance and your privacy into decision making on your financial transactions, because your financial institution and or professional may not.

Appendix A: Asset Valuation Questionnaire

Dear MYCLIENT:

We're at a point in the Risk Assessment process where we need to talk about the value of your assets. I'm going to ask you hard questions to get you thinking about Risk and Loss. The more accurate you answer in terms of real $$$, then the less FUD (Fear, Uncertainty, and Doubt) will surround the next stage of your decision making process. The less data you provide = more FUD come decision time. So it's up to you. Here are the questions.

Part I - System availability

1. Can you accept companywide downtime, or unavailability, in these systems you consider Assets?

A) Customer Loan Database (i.e. database is deleted)
B) Email (i.e. Exchange and all email stops)
C) Server (i.e. takes everything down)
D) Internet (i.e. credit reports & email)
E) Branch operations (i.e. what happened 2 weeks ago)

2. If you can tolerate even brief outages in A-E above, write down the time in hours or days that would be acceptable for each.

A)
B)
C)
D)
E)

3. Assume you lost access to the assets above. What would it cost you per hour, or per day, in terms of revenue? (It might help to think in terms of loans you wouldn't close. Does it vary with the time of the month? If so, base your numbers on the worst possible time of the month for outages.)

A) per hour- per day-
B) per hour- per day-
C) per hour- per day-
D) per hour- per day-
E) per hour- per day-

Part II - Theft, fraud, and legal

4. What would it cost you if someone "took" a copy of your database (i.e. your customer list)? What would it cost if it was being provided to a competitor?

5. Could someone (i.e. employee, customer) modify an existing database file for financial gain? How would you know it's been tampered with?

Asset Valuation Questionnaire (cont.)

6. A customer files suit for $500,000K after learning his SSN, DOB, assets, etc. were emailed in plain text across the Internet increasing his risk of identity theft. What would it cost to defend the legal action?

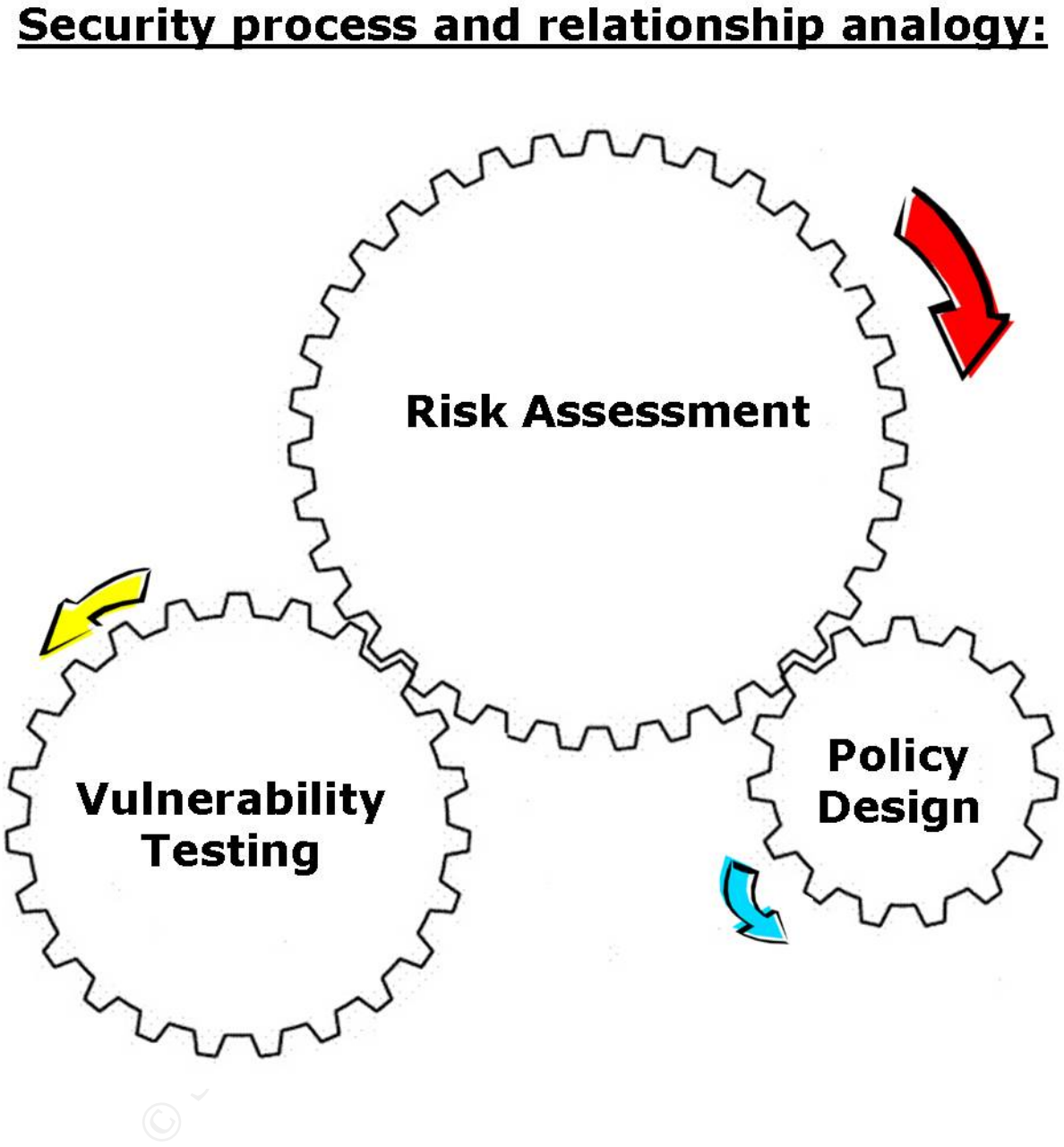
7. Would your insurance company defend or indemnify you if they discovered you weren't in compliance with Federal Privacy and Safeguard laws? Do they require compliance as part of their policy?

Part III - Loss in confidence

8. Given your marketing presence, what damage would the following security incidents cause to your reputation and consumer confidence in your company? What if there was a newspaper or TV report about the incident? Could you estimate the cost of the damage?

A) Email virus made the network unavailable for 2 days.
B) Contractor (i.e. cleaning company) stole your database and sold it.
C) An employee sold your database to a marketing company.
D) A customer had his identity stolen, $10,000 in fraudulent purchases incurred, and the breach was traced to your company.
E) A nasty internet Worm deleted your database, and you were unable to recover the database from your tape backup. Widespread rate locks were missed, purchases fell through, etc.

Appendix B: Security Process Model



Appendix C: References

1. Roberts, Paul. "FBI Warns of Spike in Identity Thefts." PC World. July 21, 2003. URL: http://www.pcworld.com/news/article/0,aid,111666,00.asp (6 Mar. 2004).

2. Kocher, Paul C. "RSA Laboratories' Crypto Bytes: Breaking DES." Volume 4, No. 2 – Winter 1999. URL: http://islab.oregonstate.edu/koc/ece575/rsalabs/crypto4n2.pdf (6 Mar. 2004).

3. Federal Trade Commission. "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act". July 2002. URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/glblong.htm (6 Mar. 2004).

4. Federal Trade Commission. "Getting Noticed: Writing Effective Financial Privacy Notices." October 2002. URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.pdf (6 Mar. 2004).

5. Federal Trade Commission. "Financial Institutions and Customer Data: Complying with the Safeguards Rule." FTC Facts for Business. September 2002. URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/security.pdf (6 Mar. 2004).

6. Loomis, Angela. "Auditing Web Applications for Small and Medium Sized Businesses." SANS Institute 2003. URL: http://www.sans.org/rr/audittech/Angela_Loomis_AT.pdf (6 Mar. 2004)

7. Bong, Kevin M. "Conducting an Electronic Information Risk Assessment for Gramm-Leach-Bliley Act Compliance." SANS Institute. May 30, 2003. URL: http://www.sans.org/rr/papers/index.php?id=1053 (6 Mar. 2004).

8. SANS Security Essentials and the CISSP 10 Domains, Track 1, ILOT 9/23/03. Section III, Chapter 18, "Risk Management and Auditing." February 14, 2003: 830-865.

9. FFIEC Information Security Examination Handbook. "Audit Booklet – August 2003" URL: http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf (6 Mar. 2004).

10. SANS Security Essentials and the CISSP 10 Domains, Track 1, ILOT 9/23/03. Section II, Chapter 7, "Defense in Depth." February 20, 2003: 293-308.

11. FFIEC Information Security Examination Handbook. "Information Security Booklet – December 2002" URL: http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/information_security.pdf (6 Mar. 2004).