Global Information Assurance Certification Paper

An Introduction to Internet Banking Security and Regulations

By Brian Berge
November 22, 2000

"Well…I understand what you're suggesting, however, at this time, management has made the business decision that the cost of implementing your suggestions is too high and not practical based on our environment." As a security consultant, I have heard these words (or some variation thereof) time and time again and the basic message generally remains; top management does not want to disrupt their financial bottom line or their day-to-day operations with the implementation of additional security measures. However, unlike the general population of under regulated corporations, financial institutions are not only looking for ways to improve their IT related security, they are paving a road that will more than likely eventually be followed by many other industries (thanks in large to regulatory agencies).

As the driving force behind the development of financial institution Internet security, the regulatory agencies all belong to the Federal Financial Institutions Examination Council (FFIEC)[1] and individually focus on different aspects of the overall financial institution industry makeup (e.g. the NCUA focuses on credit unions while the OCC focuses on banking). The agency currently leading the way and requiring the greatest level of compliance with respect to Internet banking is the Office of the Comptroller of the Currency (OCC). The OCC has issued the following regulation regarding Internet banking for national banks:

> "A national bank may perform, provide, or deliver through electronic means and facilities any activity, function, product, or service that it is otherwise authorized to perform, provide, or deliver. A national bank may also, in order to optimize the use of the bank's resources, market and sell to third parties electronic capacities acquired or developed by the bank in good faith for banking purposes."2

To "provide guidance to national banks, service providers, software vendors and bank examiners on procedures for supervising banking activities,"[2] the OCC published a document entitled "Internet Banking, Comptrollers Handbook."[2] It basically established the scope of what will be reviewed from an Internet security standpoint. The handbook contains information regarding topics ranging from growth within the Internet banking industry to firewalls and cryptography.

In addition to the handbook, the OCC has published numerous bulletins, advisory letters, and alerts with the purpose of providing "information to banks and examiners on areas of continuing concern and advise bankers and bank directors about activities and situations that could affect the safe and sound management of their banks."[2] The issuances address wide ranging Internet banking topics such as distributed denial of service attacks, certification authority systems, and privacy laws and regulations.

A recent bulletin entitled "Infrastructure Threats – Intrusion Risks", for example, addressed the hot topic of intrusion detection and contained information such as suggestion regarding the development of an intrusion risk assessment plan, controls to prevent and detect intrusions, intrusion response policies and procedures, and sharing information through the use of a

CIRT/CERT.

Those of you reading this document may be saying to yourself, "this is nothing new, every industry has a set of standards/best business practices to follow." True. However, unlike many industries, the regulatory agencies have a lot of influence over financial institutions, to the point of having the authority to issue a cease and desist order thereby closing the institution down. (As the saying goes, they carry a BIG stick).

The ability to close down operations has been good for the general customer in the past by limiting the amount of risk that we as individuals are exposed to with respect to the capability of our financial institutions being able to safeguard the assets we deposit. It has provided financial institution management with the proper motivation to address security seriously. With the relatively recent development of the current Internet banking environment over the past few years, the regulatory agencies have increasingly scrutinized the capability of institutions to protect the availability, confidentiality, and integrity of both customer and bank accounts/information from an IT standpoint, also very good for the customer.

The concern regarding Internet banking and the involvement of the regulatory agencies is for good reason. Consider the implications should a database of critical customer information, or further, consider how you would feel if it were your bank's security that was compromised. A small but visible example of the compromise of Internet banking security is through the defacement of banking web sites by crackers (defacing a banking web site constitutes criminal activity punishable by law). The web site www.attrition.org[3] contains a database of hacked and defaced web sites, including many banking sites that have been compromised. Some of the web site defacements are basically harmless and are simply a message basically saying "I was here." However, other attacks on the web site content are much more malicious, such as the one below:

> HAHAHAHAHAHAHAHA! H4K3D By Xhostrile !!!!!!!, leader of www.cyber-strike.com.
>
> Greets to Ouiji,opt1k, IL, bLaCkWinD, Hyper Viper/Silicon Toad and HDC, MetalTung, Delirium and SIN, m0f0, m1crochip and f0rpaxe, vent and L7, network weakness, Zyklon, zmonkey, xSuiCidEx, Tophat/Jouser and mobsters/sys7, Redemption, rewted, phumpy and everyone else.. oh, and h0ldkutta
>
> Special greetz to my mate Devil-c(icq#:7373443)
>
> I destroyed you page, because I hated it. Good luck rebuilding it. hu ha hu.
>
> WARNING :I stole you creditcard database. You will get it back as soon as you pay me $120.000 . e-mail me if you want to know when you must give me the money, and how. And if I find out you call the cops, I will give all the info I stole to everybody I know!

Unlike the relatively harmless attacks where the cracker simply places a message on the site

indicating that he/she was there, the above attack clearly is much more sinister and must be taken seriously weather or not the cracker was able to accomplish what the message says.

However, to nobody's surprise, crackers are not limiting their attacks on banking web sites to simply defacing the content of the site. A recent attempt to breach the security of financial institutions occurred in the UK[4]. The crackers were attempting to obtain funds through attempting to secure fraudulent loans and establishing accounts with free overdrafts. Luckily, the financial institution, Egg (a purely online financial institution and a subsidiary of Prudential), had cooperated with local law enforcement agency and implemented an application that operated proactively with respect to intrusion/detection measures. After tracing the unauthorized activity back to specific addresses, police raided the cracker's houses and seized the equipment utilized to perpetrate the attack. However, as one observer commented, it was really "an old-style fraud committed by people without enough technical knowledge to mask their identities and hide what they were doing from the bank's monitoring software."[5]

The above are just three examples of attacks perpetrated against financial institutions; certainly there have been many others. The regulatory agencies are attempting to be at the forefront of the ever-changing industry and provide financial institutions to provide the institutions with requirements that will provide protection for both the assets of customers and the institutions themselves. As the industry is growing, so is the capability of the regulatory agencies ability to perform adequate reviews. Additionally, due to the heavy oversight, and requirement to comply with regulations, the financial institution industry is, on the whole, further along than are other companies not requiring the same level of security.

Unlike the general company, that may or may not be receptive to security related suggestions, financial institutions are generally very receptive to improvement suggestions. Additionally, due to the fact that regulators review the reports of 3rd party auditors and security consultants, when suggestions are made, management rarely responds with the response that it will cost too much or is not applicable for their environment. (Little did I think that I would ever be grateful for a regulator of any type!)

References:

[2]http://www.occ.treas.gov/netbank/ebguide.htm (no specific author cited)
[3]http://www.attrition.org/mirror/attrition/2000/01/01/www.mid-southern.com/
[5]By Lucy Sherriff. URL: http://www.theregister.co.uk/content/1/12822.html

References utilized but not directly quoted:

[1]www.ffiec.gov
[4] By Steve Gold. URL: http://www.newsbytes.com/pubNews/00/154065.html