The Threat Environment:
Security Challenges and Financial Services Innovation

Author: Dr. Alec Shuldiner, Basel Consulting

Summary: The Internet's poor reputation for security is hindering consumer acceptance of online financial services. One cause is that the development process for such services tends to underemphasize security requirements, resulting in more fraud and security incidents online than need be. The financial services industry should change its approach to new product development in this area if it expects to win the consumer's trust for its online offerings. This article discusses the development process for online financial services and offers suggestions for improving that process with the goal of producing more secure products.

Introduction

The financial services industry, perhaps more than any other, stands to benefit from the continuing growth of the Internet. Most of its activities are already digitized, more of its products are inherently suitable for online marketing and distribution than in almost any other industry, and, ultimately, the Internet holds the promise of enormously more effective security for financial transactions of all kinds.

This last point many might dispute: the Internet is more commonly thought of as a playground for fraudsters and hackers than as an ultra-secure network. But as encryption, identification, and authentication solutions continue to improve, the Internet's reputation will likewise evolve from its current Wild West image; ultimately, it may well be seen by financial institutions and consumers alike as a more secure venue than traditional offline modes or even closed networks such as those servicing cash machines.

Along the way, however, there have been many setbacks and many more are to come. To some extent this stumbling is inevitable—this is still a relatively new and exceedingly complicated technology—but the large number of fraud and security incidents that have been encountered to date is far higher than need be and the public perception of Internet safety is, as a result, considerably more negative than it should be. This is no minor issue: the Internet's poor reputation for security is significantly slowing consumer acceptance of online financial services and thereby making failures of many projects that might otherwise succeed.

Why have insufficiently secure financial sites been brought before the public? In part because these sorts of new product launches have not received sufficient attention from bank regulators (though that is beginning to change) or other responsible authorities. In part, too, because much of the basic software used to deliver these products (e.g., operating systems for firewalls and servers) contains undocumented vulnerabilities. But the most important reason is that the current process of Internet innovation within most financial services companies—startups and established businesses alike—does not devote sufficient resources to security until *after* a new product has proven itself functionally and commercially. In order to understand why this is, and how this structural failing can best be addressed, let us look at the project development process in detail.

Managing Security

New product development typically occurs on a project basis: a functional goal is established and a limited amount of development time, funding, and personnel are budgeted to achieve that goal. That the final product must be "secure" often goes without saying or, at best, is listed as one of the characteristics upon which the success of the project will ultimately be measured. But it is a rare project indeed that begins with a risk assessment, without which an accurate determination of the true dimensions of the security challenge cannot be made. Thus, from a security perspective, the project's first step is more often than not a wrong one: security, in order to be maximally effective (and most efficiently achieved) should be built into the project design from the beginning. If it is not, several things are likely to happen:

Risk Assessment Defined

"Risk Assessment": A document describing the operational and technical risks applicable to a given product or operation. It should:
Completely define the various operational and technical areas of concern (e.g., "Access Control" or "Business Continuity Management").
For each such area enumerate the relevant risks and sort them into at least two categories: controlled risks (i.e., risks that are either minimized or hedged) and accepted risks.
A proper risk assessment not only defines the relevant risks but also assigns responsibility for control or acceptance of each one.

- The product concept may evolve without reference to certain limitations or additional functionality that security requirements might later impose. Once the product concept is firmly established, changing it to accommodate these limitations or to add functionality becomes much more difficult (not to mention expensive).
- The technical design, including software selection or development, network architecture, communications arrangements, and hardware selection, may be developed with a patchwork of security precautions, each added as the various designers or suppliers see fit, rather than with a comprehensive and therefore more effective security design. This can also make later risk assessment more complicated (and thus less likely to reflect true risk accurately) and can even introduce conflicting security elements into the product.
- External partners may be chosen without sufficient attention being paid to their ability to supply a secure solution or one that properly integrates with the security elements of other parts of the project.
- Security consciousness among project employees may be lower than it should be with the result that information about the technology will be too freely distributed, making it that much easier for malfeasants to locate the information they need in order to launch attacks on the system at a later time.

Furthermore, because the project will be evaluated primarily on what it can do, not what it can prevent, tradeoffs between functionality and security will almost always be made in favor of functionality. And in most projects many such tradeoffs present themselves.

Testing the Waters

If most projects do not begin with security concerns, at what point is security likely to be evaluated? Only a truly irresponsible (or desperate) company launches a product online without performing some such evaluation and in most projects security issues do arise in the course of development, albeit in a piecemeal fashion. But often security is not comprehensively addressed until the time has come to enter the “pilot phase.”

How a system behaves under real-life conditions is impossible to predict with complete certainty, and this is particularly true for the complicated systems usually required to deliver financial products. Therefore, a system’s suitability for commercial launch is typically evaluated by subjecting it to a series of pilot tests designed to show how the system as a whole works. These tests, if they are to provide a good indication of how the system will function when delivered via the Internet, must be conducted across a network and ideally across one that closely reflects the actual production environment which will be used to serve the commercial system. Making the transition from a system that exists inside the developers’ PCs to one that is actually operating across a network is an enormous step towards commercial operation. And it is this step that usually concentrates attention on security issues. If (!) an overall security evaluation is to be done before commercial launch, it is most likely to happen at this point.

This is much too late. After what was undoubtedly considerable effort and quite some time, the entire team—marketing, IT, operations, as well as any external partners, not to mention internal oversight committees and upper management—has reached what most probably think of as the last step before commercial launch. The pressure is on and time here is very much at a premium. A security review will likely have to be conducted at top speed and if at this stage it turns up serious issues the project manager will face an extremely difficult decision. A major revision could threaten the project itself, and will in any case harm momentum and morale. Even minor items will probably be addressed only if commercial launch is already going to be delayed for the sake of other technical or marketing changes. In most such projects security is brought late to the stage only to be rushed back off again.

The Threat Environment

That new product development is in many (though not all) instances allowed to proceed in this fashion makes sense given the current attitude of the financial industry. After all, it is difficult to guess which few projects will succeed, and for the many that do not, security expenditures will have proven to be simply good money thrown after bad. To put it the other way around, successful projects are allowed to develop in an insecure fashion because it is thought that the additional expense of patching them up once their worth has been proven is, in total, cheaper than the expense of doing security right for all the projects, success and failure alike, from the ground up.

This may be true, but then again it may not. For most businesses in this sector this is an untested assumption and it may well be the case that for some, perhaps even for most, careful investigation of the costs associated with new product development would reveal that the rebuilds necessary to satisfy security requirements determined upon after the project had already entered the pilot phase (or even further along) are indeed more expensive than the combined costs of ground-up security precautions for all of them, successful or not. One might also ask how many projects fail because of crippling security weaknesses detected either pre- or post-launch. In these instances, of course, all of these resources have been wasted.

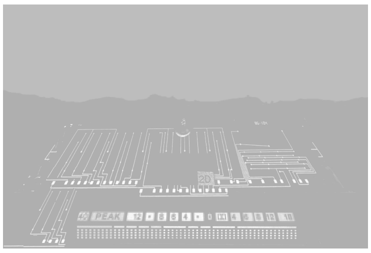
Even worse, this approach ignores one important fact: the Internet, like the Wild West of America's frontier days, is a threat environment, and in some respects an even worse one than that lawless era. The banks that the men in black hats "knocked over" contained a limited amount of money and word of a robbed bank's misfortune would spread only so far. On the Internet frontier neither is true: there is no fixed limit to the damage that can be caused by a serious hacker nor any end to how far the bad news can travel. One major incident can blow all the averages.

Improving Projects

Improving the new product development process is arguably the singe most important step towards improving the financial services industry's track record and reputation online. A few suggestions:

- *Pay for security up front*: Develop means of accurately estimating the security costs of proposed projects; do not overlook requirements for proper separation of functions when estimating the number of people the project may require.
- *Put your own resources to better use*: Reengineer internal security resources so that they better serve the needs of startup projects; require that all relevant projects make use of reengineered internal security resources; include these internal costs in project estimates.
- *Reward security-minded managers*: Make security a top success criterium for project managers; provide security training for them.
- *Assess risk early*: Require risk assessments for every project *before* developing a project plan for pilot testing; keep the risk assessment updated to reflect the actual plans for the project.
- *Prepare for disaster*: Create a disaster response plan as soon as the press begins reporting on a given project.
- *Foster a secure mentality*: Ensure that new product development is given a high security classification even while in the brainstorming stage.
- *Don't add weak links*: Do not work with external partners which are unable to provide risk assessments of their own relevant operations or are otherwise unable to provide sufficient documentation of their capabilities and procedures.
- *Spread the gospel*: Large financial institutions should purchase stakes in financial startups early on and use that equity to instill security as a value: *any* insecure online service, whether offered by a tiny startup or an established FI, can undermine the public perception of *all* online services.

Financial institutions will continue to offer new services online—this is all but inevitable given the potential cost savings and the novel capabilities this environment offers. But cost savings are of little interest to the end user, and even the lure of novelty will be ignored if it means sacrificing the peace of mind that is currently associated with traditional banking, insurance, and many other financial services. Slower but surer steps are what's needed to reach this goal.



Dr. Shuldiner is founder and principal consultant at Basel Consulting, a design and management consultancy focused on risk assessment, innovation strategy, and fraud minimization.

Please direct feedback or questions on this article to alec@baselconsulting.com.