

What Every Product Manager Needs to Know About Security

A White Paper by:

Phil Burton

Senior Principal Consultant & Trainer, 280 Group LLC



The Product Marketing and Product Management Experts™

About the 280 Group...

The 280 Group LLC provides consulting, contractors, training, certifications, books and templates to help companies define, launch and market breakthrough new products. For more information or a free consultation call 408-834-7218 or visit their website at www.280group.com. To receive future white papers like this one or to subscribe to the free 280 Group newsletter visit <http://www.280group.com/newsletters.htm>.

Copyright 2010. 280 Group LLC. All rights reserved, including the right of reproduction in whole or in part of any form.

Why Security Is Important For All Products

In the past year, online user *privacy* has become a very important topic and a major source of user concern. While computer *security* has been a long-standing concern, few product managers understand how user privacy can only be guaranteed with effective security on their company's website. As recent events have demonstrated, a company's brand depends in part on users' perceptions about privacy of their data. *Thus, if a company gets security wrong, its brand can be negatively affected. And you as the product manager can also find your career negatively affected.*

Put simply, privacy is the ability of a user to decide and control how their personal data is shared (or not) with either individuals of their choosing, or everyone on the entire Internet. Effective privacy requires effective policies in all three of these areas:

- Business decisions that protect user privacy
- User education about privacy issues and threats to user privacy
- Operations and administration practices that ensure user privacy by testing all features and defending the website against hackers.

Classically, security is used to protect a company's network, its databases and key applications, or an individual consumer's home PC and network. Typical examples include controlling access to the corporate network and scanning all incoming emails for malicious attachments ("malware.") For individuals, security also protects their email (malware that could steal their bank account login and password information), and infect their systems with viruses. Security technology also ensures that credit card information is protected during online purchases.

This White Paper will give a few examples of mistakes that companies have made, and will also demonstrate that the brand damage from these mistakes is very real. We will wrap up with some recommendations for actions by product managers.

Privacy Issue 1: Business Decisions That Don't Protect User Privacy

A company whose business model "monetizes user's private information" will often not be diligent about protecting user privacy. Google bills Buzz as a way to, "Go beyond status messages, Share updates, photos, videos, and more. Start conversations about the things you find interesting." When Google first launched Buzz, if you signed up for Buzz, Google also automatically signed you up to follow, Facebook-style, all the people in your contact lists. Through an algorithm Google also selected people with whom you did the most email and chat sessions and also included them in your follow lists. They did this **automatically**, without any input from you. Further, this information was made part of your public profile. Again, **automatically** and without an opt-in process.

Google derives most of its revenues by serving up personalized, targeted ads, and so it would seem logical that Google would encourage the growth of email and chat messages that flow through its

website. Because Google did not consider the privacy issues involved, the blogosphere was soon filled with critical comments and Google was forced to change their default privacy settings for Buzz.

On March 15, 2010, a New York Times “Bits” column, “A Blurring Line: Private and Public,” commented that Buzz was a “complete disaster” by linking email accounts to status updates on social networks. This same column was also critical of Facebook’s then privacy policy of making member information public by default. The column also noted that the issue is a “broader muddying of the line between what is private and what is public online.”

Privacy Issue 2: Lack of Effective User Education

On February 11, 2010, “Jane” sent a message from her LinkedIn account to the SunAlumni Yahoo group that read in part:

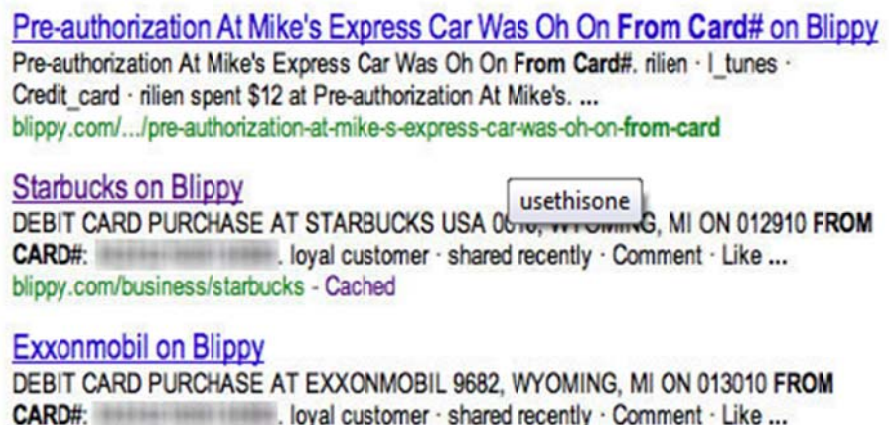
I'm sorry to bother you with this odd request. I am in a terrible situation right now and I believe you are the only one that can help me out. I am stuck/stranded in United Kingdom due the fact that I was robbed in a Gun Point. My wallet, bags, cash, credit card and my cell phone was collected at that point. It is such a crazy experience for me because I need an urgent help to fly back home. Also, the authority is not 100% supportive but the good thing is that I have my passport with me. Please, I need you lend me some money for me to get a flight ticket back home and I will refund you as soon as I am back home.

This message is obviously spam, because the story is not plausible, as several members of the SunAlumni group pointed out, and because the broken English is often a tipoff that this message came from an Eastern European fraudster. But the real issue here is why LinkedIn, in this case, didn’t provide more effective help to members to minimize the risk of getting their account hijacked.

Privacy Issue 3: Poor Operations and Administration Practices

A new website, Blippy, www.blippy.com accidentally published private credit card numbers of its members along with the details of their purchases, when it was first launched, as shown in Figure 1, according to a news item posted at <http://techie-buzz.com/tech-news/credit-card-numbers-of-blippy-users-show-up-on-google.html> (April 23, 2010)

This kind of privacy violation was almost certainly a result of a rushed schedule, because management did not allow sufficient testing and a thorough security audit



before the site went live.

Blippy promotes itself on its homepage as, “A fun way to discover cool new stuff people are buying. Blippy is a community of people helping each other discover interesting things by reviewing & discussing.” It is highly likely that an error such as the one they made will mean the end of their company.

Another example occurred in May, 2010, when it was widely reported Facebook had a bug that allowed users to view their friends’ *private chats* and pending friend requests. Thus all of what you thought were private conversations could be accessed by anyone. Whatever your view of Facebook’s privacy policies at the time, making private chats public was not the result of a policy decision. As in the Blippy example, this function went live without sufficient testing and without a well-thought out security policy.

The Brand Damage Consequences of Insufficient User Privacy

Adverse publicity about privacy issues has recently caused Facebook some well-publicized embarrassment, forcing them to revise their privacy policies and user profile defaults. But considering that Facebook has recently passed the 500 million member mark (as of this writing), it would be easy to conclude that adverse publicity has no lasting impact on the brand. However, this may change if they continue to intentionally and unintentionally release their user’s data.

A report issued in July, 2010 by a market research report released by Foresee Results, demonstrates the opposite. Their “Annual E-Business Report for the American Customer Satisfaction Index (ACSI)” ACSI measures 223 companies (including both online and offline companies across all economic sectors and industries).

This report contains the startling finding that out of all these 223 companies, only 10 score a 65 or below, including Facebook and MySpace, which puts them in the bottom 5% of all measured private sector companies. The other companies that join Facebook and MySpace in the bottom 5% are all airlines and cable companies, which are two perennially low-scoring industries with terrible customer satisfaction. [*Italics added for emphasis.*]

In assessing their research results, Foresee Results notes that, “When asked what they like least about Facebook, survey respondents gave answers including, “privacy and security concerns, ... spam ... “ Foresee goes on to warn that, “Should MySpace stage a comeback, or should any other competitor to Facebook deliver a truly superior customer experience, Facebook should have cause for concern.”

Facebook’s business model is based on the willingness of its users to disclose personal data about themselves, which can then be analyzed and sold to marketers seeking to target specific customer demographics. For example, see these blog posts:

- http://blogs.hbr.org/cs/2010/05/facebooks_culture_problem_may.html
- <http://lastwatchdog.com/facebooks-business-model-hinges-wiping-privacy/>

If users become less willing to disclose their personal data on Facebook, then its revenue will suffer. And if your products suffer from a disaster such as these your career can be adversely affected.

Your Role as Product Manager

As the product manager, you are in a unique position within your company. No one else has the same broad overview of the entire business situation of your product as you do. Not engineering, not sales, not finance, not operations. With that perspective also comes responsibility.

It is your responsibility to define the market problems and issues. As the product manager, you don't build and deploy solutions. That is the job for engineering and operations.

In this case, the market problem is user requirements for privacy. The solution to privacy requirements is effective security, a combination of

- Company Policy
- User Education Programs
- Programming and Operations Excellence

Here are a few things to consider:

- Do you have requirements for how your customer information is stored and used?
- Do you have a written privacy policy on your website?
- What security is implemented to protect the data of your customers?
- What is the escalation path if your company does accidentally release private information?
- Are there any processes in place to audit what information from your company is being published on the web? (For one of our clients we found their competitor's confidential price list on the web doing a simple Google search)

Your job, your challenge, your opportunity, is to define the requirements that lead to effective solutions in these areas.

How the 280 Group Can Help You

Security and privacy can't be viewed as an afterthought to your product or service – the resulting damage could be fatal to your company *and* to your career.

The 280 Group specializes in product management and product marketing and has dedicated consultants in the security area. We can help you put together a plan to ensure that your brand and products are adequately protected. We can also do a privacy audit for you and come back with specific recommendations and requirements that you can include in your product and company planning.

Next Steps

This white paper has discussed security and privacy issues for products. For in-depth additional information or a free quote for a security and privacy audit for your products contact the 280 Group at contact@280group.com or (408) 834-7518.