Failed:

Information Security and Data Protection in a Consumer Digital World

Rafal M. Los

Information Security | Data Protection | Risk Management

http://PreachSecurity.blogspot.com

Information Security is in deep, deep trouble. Computer users are apathetic to the rampant theft of information and identities, and the issue has become background noise in the news.

As insane as that sounds, ask someone who regularly reads the media when the last time they read about information theft was… then ask them their reaction. Perhaps the thing that should shock you more than anything is the fact that John and Jane Consumer just don't care – they've become apathetic to the mountains of news articles and media hype around information theft, identity theft, and fraud going on in the digital world.

Every day we hear about it on the news, read about it in the papers, get it in our RSS readers, and talk about it at the water cooler. Stolen identities. The bad news is everywhere and unfortunately… people are starting to dull to it. The problem is that the shock value of people's identities being stolen is starting to wear off.

> *Before I continue on this topic, I feel it important to point out that I have a slightly different view on information security/data protection and the purpose of the profession. My contention is that information security professionals are fighting the wrong war; or rather, for the wrong cause. We approach security from the viewpoint that there is an absolute, or a state of "security" where we feel there is no risk of the negative. This state of mind is completely wrong. In fact, I will take it a step further and say that the goal of information security/data protection isn't to "win" the battle [against the "bad guys"] but rather to stave off the enemy from the castle keep for another day. This distinction is important to keep in mind as the rest of this paper work from that frame of reference.*

Let's look at what my research has shown to be the five main causes of information protection failures, and address them each on their own – and think about how information security can react to counter the negatives. For the sake of simplicity I will use "Information Security" as an all-encompassing term for the groups which comprise data protection, information security and risk management in the business. There are many other names for these groups, but these are the most common.

The Five Reasons for Failure

The five most prevalent reasons for information protection failures in recent history are as follows, in no particular order:

- Consumers opt for simplicity over security
- Decentralization of data storage
- Consumerization is driving the adoption of unsecurable technologies
- Information protection has fallen victim to "passing the buck"
- Consumers still don't understand the impact of information compromise/theft

Of course, there are other reasons why there are cascading failures all over the news and across board rooms from sea to shining sea to the land of the rising sun and everywhere in between. These have shown themselves to be the most obvious, the most cited and the most problematic.

These issues are very serious, and must be addressed because they are creating an environment where apathetic users are clashing with overmatched information security teams; and thieves are benefitting from the chaos and confusion. Only after we [information security professionals] are armed with the appropriate knowledge and facts can we truly start to make headway to solving this information crisis. Information theft, identity theft and the resulting fraud won't simply stop on its own – the benefits are simply too tantalizing, so something must be done.

Addressing information theft, identity theft and the resulting fraud is a monetary problem. Thieves aren't in this game for the fame, or the glory. They're in it for the cold, hard, cash. Thieves are all about making money so in order to begin to match them on the field of battle we the information security community must capture their perspective, and understand their mentality. We must also take as our own the views of the average user of any system we are attempting to make more secure – because as I will shortly point out the most secure systems are the ones no one wants to use.

I. Consumers Ops for Simplicity Over Security

At what point did technology leave behind the K.I.S.S. principle? This principle taught us to Keep It Simple Stupid, and it's worked very well for years in the non-technical, non-digital world but for some reason it's having a very difficult time translating into the digital everyday.

Perhaps it's because simple is the arch enemy of secure? I don't think so, since there are many systems which are simple yet very secure. Take for instance… or no, wait… hrmm… OK so I can't come up with a single thing that's simple and secure. In fact, I can't think of anything right now that I would consider "secure" or even relatively secure that isn't complex. Everything from a credit card, to online banking is becoming more and more complex as security rears its head. Logging into a computer used to be as simple as turning it on, and starting work. Then came the username and password, but of course that wasn't secure enough, so we've now moved past that to digital fingerprint scanners, smart-cards and other gadgets which make working with computers for anyone who didn't grow up with an Amiga overly complex. The reaction of most people is to remove any trace of security and simply opt for usability… this should scare you.

Sociological theory teaches us that the standard reaction for something that makes life difficult is to simply throw it away, or opt for simpler solutions. Human beings prefer simple, this isn't rocket science and you don't need a PhD to understand this concept. Since it's not so easy to simply cut up your credit card and use cash (which is significantly more "secure") online throwing away the credit card simply isn't a realistic answer. The reaction them becomes to move to a technology or product which is "easier to use". Notice the distinct lack of "and more/equally secure" in that description. Banks who "over-complicate" the logins to their online sites often find their customers signing up and moving their accounts over to a bank which doesn't have all that fancy security gadgetry. This type of reaction for security and data protection professionals is simply unconscionable. Why would anyone in their right mind convert to a system that is less secure? The answer is quite simple… and painful to hear – it's easier to use. There are other reasons as well which make this type of reaction feasible for end-users, a topic which will be covered in point four.

While this may be obvious to some, the question remains on everyone's mind – what to do about this problem. This is a very real problem which must be addressed otherwise all the security in the world won't do any good if it's countered by user migration to insecure systems.

The answer to user avoidance of higher-security systems is to create higher-security systems which are comparably simple to those low-security systems; with the added benefit of being secure. Until now it's been an accepted fact that good security comes with the complexity penalty – but as a community of professionals we must come up with a way to address this issue. Some certain businesses are already starting to come up with innovative ways to make the end-

user more secure without increasing the complexity of their daily lives, but the message isn't getting out fast enough. More must be done. Business must start to adopt the herd mentality for the common good, start to center around end-user simplicity while building in higher-grade security truly transparent to the user.

Several approaches to advanced security without the complexity penalty have already been established and are presently working in business. For example, Bank of America's online system is little-more-complex than a simple password mechanism but adopts many back-end analytics and advanced security technologies which are entirely transparent to the user such as IP address profiling, behavioral modeling and other key features which ensure user security without complications to the end-user. This type of situation is a win-win and not only drives better security but increased trust in the particular business, in this case Bank of America as a trustee of critical information.

If you've read carefully, I mentioned that we must create higher-security systems which are comparably simple to the less-secure ones… this is a very deliberate wording. Even in the best-case scenario there will be some *complexity penalty** for the added security. This is alright, as long as it's still "simple enough" for users to continue to use the system – this requires user testing in a sample size big enough and encompassing enough to gauge real-user reactions… from real-world scenarios.

The realities are clear – users will opt for simplicity over security almost every time. While this often puts functional designers and security experts at odds, it should be the uniting factor in the war against information thieves.

**I will address the concept of the "complexity penalty" in a later publication, as this requires a significant amount of space on its own.*

II. Decentralization of Data Storage

Another clear reason for the cataclysmic failures in information protection is the massive disbursement of information. Over time, information migrated from single-source such as a floppy disk or a hard drive which was relatively simple to secure to complex distributed systems such as Microsoft's DFS (Distributed FileSystem) or worse-yet the ethereal space known as the

"Internet". The advent of the Internet has set information protection back into the Stone Age. All the years spent securing centralized data stores has been for absolutely naught, since there is no such thing as a centralized enterprise data store anymore. Look around in your place of business… you will find critical information on laptops, desktops, servers, network storage appliances, file-servers, web-servers, USB devices, iPods and countless other devices moving through your networks every single minute of every single day.

The obvious issue here is one of locality. How does one erect a virtual wall around an indescribable perimeter? That thought has perplexed many a great security architect, and it appears even the greatest minds are still failing to account for every possible human stupidity. It's not enough to account for the legitimate uses of data and data storage devices – accidental and malicious use-cases must also be accounted for. This seems more like a losing proposition every minute, doesn't it? It seems that even though the data perimeter is infinite, the funding and resources to secure it are quite finite – I assure you.

Whether you're just seeing the light bulb go on, or have been preaching this problem for many moons you're still left in the same exact spot. You're left asking yourself… now what? It seems that there are hundreds of tools out there geared for single-user all the way to enterprise-grade solutions which aim to address this issue… one component at a time. Some vendors offer to secure intrusive USB memory sticks (in all their variations), others offer to secure mobile data stores (such as laptop hard drives), and still others will encrypt your cell phone. I challenge you to find one such strategy which covers the broad spectrum of devices, operating platforms and use-cases. There are none that I've been able to find. The challenge is open… the problem lay before us – and I unfortunately don't have a good answer.

III. Consumerization is driving the adoption of unsecurable technologies

The term "consumerizaton" has been tossed around, informally, for a few years now and if you're not yet familiar with the term back in 2005 Gartner defined it as "*practice of introducing new technologies into consumer markets prior to industrial markets*"(http://www.gartner.com/press_releases/asset_138285_11.html, 2005). What this really means is that technologies which are invasive to businesses aren't being introduced through business channels – they're finding their way into consumer hands first. The ultimate example of this "Consumerization" is the iPhone from Apple. The iPhone didn't get its start as a business device,

but rather as a consumer-marketed device which immediately flooded business networks and wreaked havoc until IT administrators and security professionals figured out what to do about it or how to properly accept it into the business.

This type of scenario is becoming more and more common. Consumer technologies are finding their way into businesses long before corporate IT has any idea how to handle them. Therein lies the problem. Devices and technologies which are not meant for the business world are finding themselves propelled into the business world because users demand it. This type of situation creates an adversarial relationship between corporate IT and IT Security and the employee. While corporate policies can dictate that no unapproved devices are ever allowed to be connected to the network – ask yourself how well that works out. We've all connected our iPod, web cam or external gadget of some kind to our corporate laptop. We're all guilty of it, let's face it. There wouldn't be a problem with this if by doing so we didn't completely compromise the security and integrity of our corporate network.

So then what? How does a corporate IT Security department handle "consumerized" technologies flooding the workplace? Policies? Locking work computers down completely? Or does the Ostrich approach seem more likely? Again, there are no simple answers here – only complex questions which merit study, investigation and extensive research. In the meantime, the only workable tactic is to try and get out ahead of the curve; to embrace and accept the upcoming technologies that will rock the consumer market as inevitabilities in the corporate space and attempt to find ways to "live with it" until we have a permanent answer. The sad fact is that business tools such as laptops, desktops and other corporate-issued devices are fundamentally flawed and incapable of handling the stringent data-protection requirements which modern business mandates. It's nearly impossible to turn off hardware access to a USB port since more often than not mice, keyboards, smart-cards and other devices must be plugged into perform meaningful work – but some devices (iPod, web-cam, etc) must be kept out… but there are no "real" ways to distinguish between an approved and unapproved devices, on an enterprise scale.

While the problem of design simply proves the immaturity of enterprise technology, talking about it is about as effective as solving math problems by drinking beer. We're not going not going to get anywhere without actions. What's needed is a very hard decision… to move away from "ultimate usability" into a model where enterprise control of devices and technology (and thereby, data) is the base principle around which technology is designed. The Trusted Computing

Initiative is/was one attempt to accomplish this – but then severe complexity stepped in and nearly killed that initiative for all but the highest-security military and business applications. The task is monumental; a fundamental redesign of hardware platforms and operating environments to serve a business purpose – not a consumer purpose – will ultimately shore up the wave of consumerization which is crushing data-protection measures.

IV. Information protection has fallen victim to "passing the buck"

If you've spend any time in corporate America you're probably well-educated on the "pass-the-buck" game which businesses play. As risk becomes the major factor for large-scale contract negotiations involving sensitive and critical data, responsibility for that risk is passed on down the line. Your doctor's office does it, your bank does it, and your online retailer does it – and you'd never know it. Your information, while within the possession of an online retailer, actually is processed by some 3rd party which then assumes responsibility (at least contractually) for that data as a result of the business model. This practice enables the primary business to "pass-the-buck" down the line and passes the responsibility for your precious data down to the next one in line.

Every business writes in a "responsibility and liability" clause into their contracts with their vendors and they in turn do this on down the line. Ultimately, the responsibility for your personal and sensitive information is passed to a party so far removed from the core business they not only have very little knowledge of security but even less knowledge of the original business intent for the information they are charged with. When a bank accepts your personal information common sense would dictate that in a court of law they are legally responsible and liable for your information, right? More often than not this is wrong. That bank likely has custodial relationships with many vendors, partners and external parties which work with that data in some form or fashion. The bank then writes liability clauses into the contracts with those 3rd parties, thereby passing the responsibility for maintaining security and confidentiality of that data to that outside party.

In legal terms this is all very legitimate – and even in the technology world this could still be legitimized if it wasn't the mentality and lack of responsibility that this practice fosters. Because the liability is now passed on down the line the originating entity or business now feels relieved of the responsibility to be …well, responsible with your data. Why should that bank spend

millions securing your personal information when they can simply write off the liability onto one of their vendors which also handles that data. Granted, the liability transfer only covers the relationship when data is actually handled by that 3rd party it's a gaping area of responsibility that's left open. This is what happens when lawyers are set loose to try and figure out how to push risk and liability off onto someone else. They're good at that – but somewhere in translation your data goes missing and no one's responsible.

V. Consumers still don't understand the impact of information compromise/theft

I can't believe that it's August 2008 and I'm writing that consumers still don't understand the impact of information theft and poor security practices. I was sitting in a room-full of thirty-somethings not too long ago, all of whom were Internet-savvy by the way, and someone asked me why their bank was so difficult to get into. "All my passwords are the same" another one added, "I don't really care if someone wants to guess my password – what would they want with my email anyway?" It's exactly this lack of understanding that's devastating to good security practice and policies. Paying the *complexity penalty* must not be a show-stopper for good security practice.

It never ceases to amaze me that consumers still freely give away their social security numbers to anyone who asks. What legitimate use for a social security number does your cell phone carrier have? When confronted with the question on a recent trip to the doctor's office the office manager couldn't come up with a good reason to ask for my social security number other than to "keep as a reference". That's just not good enough, and I shouldn't be forced to give up that information if there's no compelling reason. Up until recently some people had their social security numbers printed on their checks and their driver's license. I can't think of a less intelligent thing to do when it comes to protecting your identity. If you just happen to leave your driver's license somewhere not only will the person picking it up have your name, address, and driver's license number but also your social security number which – if you've applied for credit recently – means that they can open credit in your name.

When I open a talk with the number of confirmed stolen personal records in excess of 20 million people simply don't gasp in horror. In fact, some people have started to ask me if that number is

inflated, and how many of those personal records actually resulted in confirmed identity theft. They're entirely missing the point! What I don't understand is why the people out there who have lost their reputations, their credit-worthiness and parts of their lives to identity theft aren't making information security awareness a bigger deal. It just boggles the mind. Are today's consumers so desensitized to information loss, fraud and identity theft that they simply won't care until they spend hundreds or thousands of dollars of their own hard-earned money reclaiming their identities after an incident?

I can only surmise that there is a severe lack of education for consumers in this modern digital information society. People are living in an ever-closing world with MySpace, FaceBook, online banking and medical records management all reachable through their favorite browser; and very little protection for the precious information which governs their lives. As an industry of security professionals we must educate, educate and educate some more until consumers are fully aware and no longer apathetic to the cause of data protection and information security. I honestly feel that there is no other way to "win" the war against information thieves… but through better education of our consumers. The challenge, of course, is how do we reach them when it doesn't involve making money? Let's face it, every business model centers around making money – and the not-for-profit agencies out there aren't potent enough to mount a campaign of education like that which is needed… or at least I haven't seen one potent enough yet. Perhaps another challenge must be issued – to corporate America and non-profits everywhere… let's educate our consumers on the topic of information protection and the dangers of the online world while continuing to provide services in that digital world and driving them to our virtual doors. We information security practitioners don't stand a chance without consumer education.

As a final thought…if you the reader haven't noticed yet – there aren't any simple answers here. I've made attempts to confront some of these tough issues but sadly I feel that they will be persistent over the next decade and may even get worse before we reach some tipping point at which things will drastically change virtually overnight. Until consumers realize how precious their personal information is, and businesses start to accept responsibility for that information and actively seek to build a business strategy around protecting that information – we're doomed. Forget reaching a state of "information security nirvana"… I'll be happy if by the time I wake up tomorrow someone hasn't bought a house in my name.