MOTIVATING AND FACILITATING THE CHANGE TO BIOMETRICS

To Address Identity Theft, Privacy and Data Breaches, and Much More

People wonder why Privacy and Data Breaches and Identity Theft have become such serious and growing problems. It is easy to let these problems take center stage when they receive media attention. Yet, this is just the tip of an iceberg of security concerns. Broadly speaking, Privacy and Data Breaches and Identity Theft are part of a bigger topic, "offensive and defensive network warfare," which has serious implications for all aspects of our lives and infrastructures. Privacy and Data Breaches and Identity Theft should be considered a wake-up call that helps us better prepare for what could likely come.

Those that suffer the consequences of identity theft see that as their focus. They likely suspect that their difficulties had not been prevented because big business did not have a vested interest or leaders did not care enough. Governments are similarly held responsible. Other people think that there is no real solution, in part because technology is not ready for "prime time," but also because there have not been sufficient expenditures of time and money to make the necessary fixes. There are also those who lack concern because they doubt if they will ever be affected. They see a struggle between good and evil with neither side having a clear and decisive advantage. Still others believe that people are inherently careless and simply bring bad things upon themselves.

So should anyone be concerned enough to take action? If so, how serious should they be? Are breaches and identity theft a sufficient reason for adopting biometrics? Or are there more aspects of a complex subject that should be considered? We believe that the latter is the case and that there is much more at stake than a simple solution to a single problem. Things are much too complicated for any quick solution especially when there are tradeoffs that impact other priorities. Then how should problems be approached, and what expectations should be set? This paper is intended to help readers come to their own conclusions and decide on a reasoned and balanced course of action.

First, are things as bad as they seem?

In actuality, things are probably worse. There are many others out there interested in creating mischief besides criminals. The list includes: foreign governments, terrorists, disgruntled employees and careless individuals. All have there own agenda with specific goals and objectives. Whatever their reason, it is important to keep track of what they are doing and put an end to aberrant behavior.

We'll start with criminals.

Criminals don't just use stolen identities to create fraudulent credit card accounts in someone else's name; they also commit crimes and shift blame to these same innocent victims when they are caught.

Those committing lesser crimes know that the system will allow them to be released pending a hearing and an assumed identity will likely not be discovered. The consequence is that when they fail to appear in court to face the charges, you, the person whose identity they used, will be the one that is looked for and apprehended. Imagine getting stopped for a broken tail light and getting thrown into jail because some criminal did not appear in court! It is hard to believe, but this really happens. Furthermore, it is very difficult to clear an arrest record even one based upon a false identification.

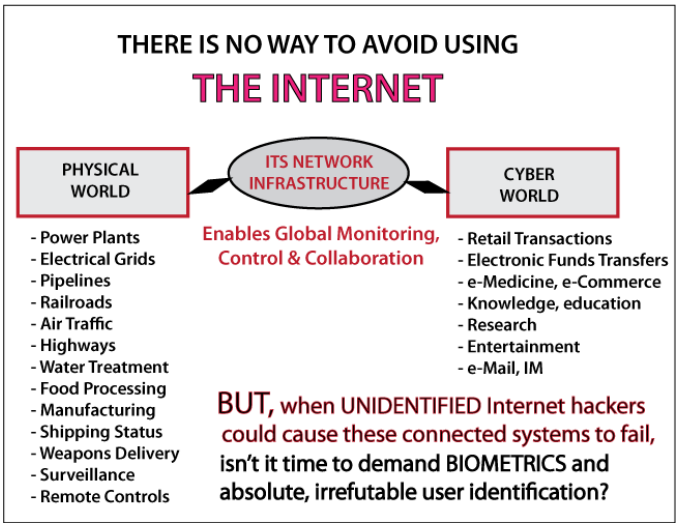
For more information on the threats that you face, visit: http://www.privacyrights.org/ar/Privacy-IssuesList.htm. You will find a wealth of scary information. In particular, look at item #7.

Remote access is a cost-effective way to avoid getting caught.

Why rob a bank and get caught when it can be done easily, conveniently and safely from a cave someplace? The same strategy applies to anyone, any government, any organization interested in doing harm with a multiplier effect. After all, who would consider risking a confrontation with a superior force if they could accomplish the same thing through offensive network warfare? The business case says that just as with the 9-11 terror attacks, a small investment can cause trillions of dollars in damage when systems and societies implode. Recognizing this is an essential first step in planning defensive measures. Even an individual can benefit and reduce exposure by turning computers off during long periods when they do not need to be kept on. It saves energy at the same time.

Anything that is connected, even wirelessly, is potentially hackable.

Sure it could take a long time, but faster, more powerful computers and better software make the job easier. Consider the exposure all around that is exemplified by the following diagram. As you look at it, consider how attack airplanes could fly into one of the most heavily protected air spaces in the world unimpeded because defensive systems had been hacked an made to not even see the attackers. How long did it take to be able to do this? And, could it be done at will or could it be prevented?



What will fix these problems?

Lack of proof-positive identification for each and every transaction is the culprit. When passwords and other circumstantial means of granting access can be readily lost, shared, stolen, forged or otherwise compromised, something better is needed. Layering different methods of authentication simply slows down those with the tools and fortitude needed to breach them. If essential information or credentials have been handed over foolishly or carelessly in response to a phishing attack, anyone can fall victim.

Conventional wisdom says that biometrics is the answer.

They are based upon physical and other characteristics of the human body that allow every individual to be absolutely and accurately distinguished from another. With biometrics, even carelessness will protect user credentials in the form of fingers, faces, eyes, etc. However, despite the long-time use of fingerprints in solving crimes and more recent media grabbing attention to successes with DNA, the potential of biometrics has largely been untapped. Let's look at the reasons why.

What is holding biometrics back?

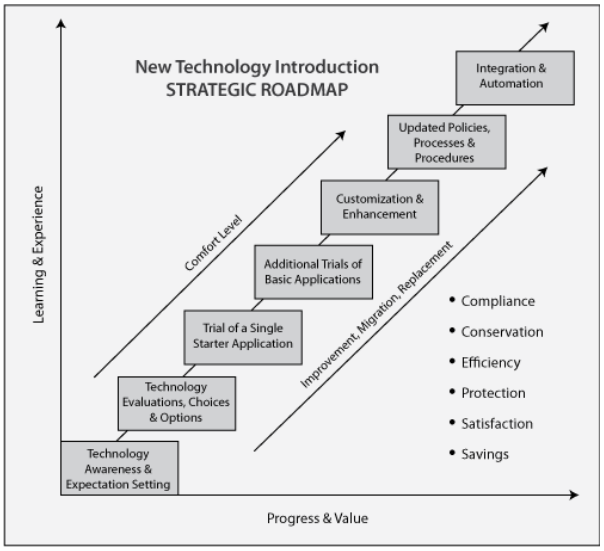
Any new technology requires a gradual period of adoption. People rely upon technology, but fear it. Even new ideas and technologies that bring significant benefits are difficult to get off the ground. They can be challenging even for the experts, and people are conditioned by past failures. Tradeoffs require careful balancing of priorities, especially when a fear of difficult implementations leads to status quo mentalities that perpetuate established infrastructures. BIOMETRIC technologies have been further encumbered by privacy concerns, poorly-understood technical complexities, products that fail to work, basic misconceptions and flawed implementations.

Imagine being responsible for spending millions of dollars on something that not only does not perform as advertised, but makes matters worse. What executive who expects a multimillion dollar bonus would be foolish enough to take such a chance if it had not been thoroughly proven under actual operating conditions. This is especially true when remediation expenses (similar to those that cover shoplifting costs) can traditionally be transferred and charged to customers. Even consumers are part of the problem when they are uninformed, do not demand more from their banks and merchants and fail to recognize steps that they themselves could be taking to help. Every delay stifles demand and discourages vendors from making the necessary investments to advance and deliver the technology, creating a vicious circle. Unfortunately, bad experiences turn into lessons learned that cause

extraordinary caution to avoid repeating them. This seems to happen over and over again with biometrics, especially when there is uncertainty about the source and extent of failures. Is it really a failure of the biometrics or a failure to successfully manage their introduction?

There is an experience curve.

Change has been gradually progressing, but it hasn't and doesn't happen quickly. It requires a reasoned, organized process that examines alternatives, gathers user feedback, considers value propositions and gradually makes changes that prove-in concepts without the risk of catastrophic failure. For change to occur, the climate must be right. People must know what to do, but be motivated to take informed action and use resources correctly to test the water before jumping in with a full commitment of funds to an enterprise rollout. Starting in a methodical way cuts the risk from going too far, too fast. Here is an approach that works well for any technology, not merely biometrics.



Biometrics, as a means of improving user identification, is advancing.

Strides have been made to improve the capabilities and value of a wide range of biometrics including fingerprints, faces, voices, eyes, irises, veins and hands. Never-the-less, the technology remains in its infancy with a long way to go before it fully protects all the identities and assets of every human being. However, without biometric identification, consumers will continue to incur spiraling costs associated with breaches and forgo related benefits including ease of use and convenience.

With greater awareness, pushed by escalating costs, greater value will be realized from "revolutionary" advancements as biometrics become more widely recognized, tested, trialed and deployed. Simple, next steps at the individual and enterprise levels will avoid having to adopt changes under duress.

Become proactive in a measured way.

Forget the expected longer-term benefits for now, but why risk having to undertake last minute crash programs? There is a middle ground between maintaining the status quo and an attempt to rollout untested solutions to an entire organization. The smart money says to stay in tune with the market, learn from others, develop a migration strategy and take a stepped, reasoned approach that focuses first on the individual. Simple beginnings bring sufficient value to justify getting started. Initial ease and convenience are accompanied by reduced frustration and time savings that everyone can use. Greater broad-based benefits will gradually follow as dots are connected, systems and solutions become integrated and component parts are made interoperable. New products and tools will help to point the way.

In summary, refer to the attachment for highlights of contrasting factors to consider. In part, they will be helpful when developing a business case. No major project should be undertaken without one.

For consulting assistance, please contact:

Rockwood Management Services
52 Johnson Drive
Chatham, New Jersey 07928-1168
973-635-1970
info@rockwood.com

SUMMARY OF CONTRASTS AND CONSIDERATIONS

FACTORS	WITH BIOMETRICS	WITH NON-BIOMETRIC STATUS QUO
Costs	Change takes new funding. There is a transition period with overlapping costs. Going too far, too fast is both inefficient and impractical.	It also takes money to maintain the status quo, but that is already included in cost structures except if reserves prove to be too low as breaches escalate. The danger is loss of a competitive edge if others adopt cost saving technologies.
Privacy and Data Security	Only biometrics provides true, trusted, absolute, alias-free user identification. It is proof-positive.	Passwords, tokens, smartcards and other commonly used forms of authentication only assume that the person who has them is also authorized to have access privileges.
Performance Management Systems	Biometric identification establishes accountability and improves the operation and effectiveness of compensation systems.	Rewards are designed for those who meet traditional goals and objectives that increase short-term profits and make investors happy. Could this structure be flawed?
Regulatory Compliance	Biometrics supports the spirit of true compliance, not just the letter of the law.	Current best practices set minimum standards creating a financial incentive to stay within them.
Accountability	Accountability improves with forensic logging, tracking and control.	Systems can be built around Financial Accounting Standards that are designed to pass audits.
Learning Curve	Small steps focusing on individual users gain experience and avoid throwing money at problems later.	Technical personnel lack the time, experience and motivation to take on more roles and responsibilities.
Security Breaches	Customers benefit from lower costs; companies benefit from greater competitive value and profitability.	Businesses simply recover costs that competitors also incur. Some are lucky and avoid costs altogether.
Transitions	Careful planning will avoid the shortfall from either extreme.	