Identity In Security: The Problem With Billy

PROMO

The Walsingham Institute

Table of Contents

Disclaimer
This report, “Identity In Security: The Problem With Billy”, provided by The Walsingham Institute Inc., contains an analysis of the perspectives, issues, challenges and consequences related to the use of identity in security measures. This report is intended to serve as an educational tool to assist in achieving a better understanding of identity as a basis for developing security measures. As such, this report is to be used for general reference purposes only and is not to be construed as legal advice. The purchasers of this report are responsible for ensuring that the use of identity in security measures is in accordance with the laws and regulations to which they are subject.

Overview & Highlights

Overview:

In this Walsingham Report we consider the concept of identity and its use as a basis for select security measures. Through the creation of a character, Billy Schumacher, the concept of identity is deconstructed and analysed. With an understanding generated from this analysis the role of identity is considered when applied to Border, Perimeter and Corporate security measures. As always with Walsingham Reports, this document is interactive and best read at a computer connected to the Internet.

Who should read this?

"Identity In Security: The Problem With Billy" is a primer on the concept and applications of identity in security and is meant to question current approaches to increasing security. This Walsingham Report is intended for anyone considering the use of identity as a basis for security measures.

Highlights:

Identity is a fluid concept that builds and changes over time. Moreover, identity is extremely difficult to authenticate definitively. Thus, the most effective security measures that use identity as their base are those measures, which are limited to a finite number of users. Indeed, the fewer the individuals being identified the more capable the system. Thus, applications of identity in corporate management systems and perimeter security are far more effective than those used in border security.

Biometric identifiers are perhaps the only reliable method currently available by which we can quantifiably measure a person's uniqueness with a high level of accuracy.

Security approaches relying on identity are not viable preventative measures, particularly in widespread applications. Understanding human behaviour as a means to uncover or predict intent should be the focus of any security measure involving people.

A security measure, whether proposed or existing, that uses identity as a base needs to be revisited from a holistic perspective; considering not just the individual measure but also the wider concept of security.

Identity In Security: The Problem With Billy

Having an identity is a person's ticket to partake in all a social system has to offer - collect a pension, drive a car, receive health care, travel, bank, vote. It is also a possible ticket to some assurance of security. But what is it about identity that affords it such an integral role in our lives? Does having an identity really make us more secure?

Humans have been struggling to define identity since first perceiving themselves as separate beings. apart from nature. The need to understand what makes someone unique or different, and to accordingly establish enduring categories has been compelling and open-ended.

What is Identity?

Identity, in its simplest definition, is a set of traits, by which an entity can be distinguished from others. Depending on the field or interest – identity can take on a variety of forms. Some definitions are more rigid – logicians feel identity can only be in relation to an object and itself – while other definitions focus more on function – as is the case with the field of computer science and object-oriented programming. Companies are concerned with corporate identities, whereas Internet users are concerned with the way they would like to be represented in a digital realm through the creation of online identities. Although these concepts of identity are important to many, perhaps no other type of identity affects the lives of more people than that of personal identity.

Personal identity is a concept that builds up over time. Characteristics that can serve to distinguish one individual from others are noted and collected to create such an individual's identity. There are roughly five predominant trait categories that are used when establishing and tagging an identity: Personal, Mental, Physical, Social and Bureaucratic. In the collecting of data on which an identity is built in most cases begins before the individual is even born.

Personal Traits

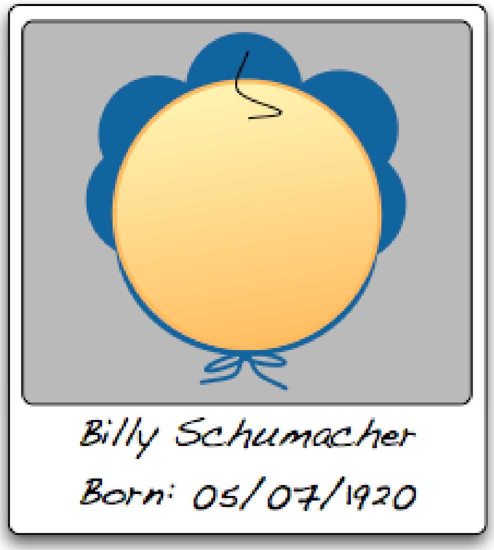
Many characteristics associated with personal data are assigned to an individual before they are conscious of themselves. Given names are often selected for the child in advance of their arrival. Traits that are passed on through inheritance such as ethnicity or surnames are predetermined based on an individual's parentage with exceptions in the case of adoption. The language a child learns to speak first, or mother tongue, is as the term suggests a lingual transfer from parent to child. Even religious identifications tend to arrive from the education of children by their parents.

Take the example of Billy Schumacher. When Billy arrives in the world a great deal regarding his identity has already been established. Billy has a full name, a date of birth, ethnicity, a nationality and most likely a religion. Billy is the possessor of an identity before he is even aware of what an identity might be.

Names

Although names were at one time conveyed descriptions of a person's physical attributes or skills and as such unique labels used to identify individuals, names today seldom define the persons referred to by them.   It is doubtful that Billy Schumacher is so named because he is a *wilful protector* who *makes shoes*. Indeed, it is more likely that his father's surname was Schumacher and his parents preferred the first name William enough to call their son knowing that he would most likely be called Billy. Just as likely, a person can choose a new name by which to be referred.

Nevertheless names, both given and inherited, are most commonly the primary attribute from which identity is built.



Ethnicity

Based on a combination of a person's mother tongue, the ethnicity of his or her parents and sometimes their religion, a sense of cultural identity is created. Yet what makes one group truly distinct from another? As the world population has grown, so too, apparently, have the number of differences between people. Despite this, DNA tells us we all share common ancestors. There are only a finite number of linguistic roots from which all modern languages have derived. The fundamental teachings of most religions have the same principles. Even similarities between cultures are at times startling. What many perceive to be clear, permanent distinctions differentiating their group from other groups is often just a matter of opinion. Indeed, an outsider would be hard pressed to distinguish a Serbian from a Croatian, and likewise a Croatian from a Bosnian unless the distinction is drawn by the Serb, Croat or Bosnian or a religious rite is performed thus providing a demonstrated difference between the three.

It is around these ethnic distinctions that many add to their foundations of identity – ascribing similarities of a wider group with their personal identity. In a sense, a person creates his or her identity from perceived similarities they share with others yet at the same time realizing that there is a separation – a sense of self.

Mental Traits

By the time Billy becomes aware of himself as a separate individual, he will have already amassed a considerable number of traits which he will use to identify himself throughout the course of his life. However, none will be so difficult to verify nor as essential to Billy's sense of identity as the mental attributes he will develop over a lifetime. Awareness, experience and memories are arguably integral traits of personal identity.

In understanding that he is Billy, young Mr. Schumacher becomes conscious of himself. He perceives his identity. Over time his experiences and the memory of those experiences build up and shape his identity. It is in this concept of self that a person may realize that one can be truly responsible only for oneself – as the only actions Billy can realistically control are his own. In many ways, it is through the development and fostering of such personal self-awareness that true security can be achieved. For only when a person understands that he or she alone is in control of his or her actions or reactions that responsibility for the consequences of those choices is comprehended and accepted. The responsibility for one's actions from each member of the group is transformed into security for the whole group.

Unfortunately, unless someone can read Billy's mind these mental attributes are highly dependent on what Billy alone claims them to be. The reliance on memory and consciousness to build identity renders mental traits unreliable. Indeed, as a means for self-distinguishing in front of others, mental attributes are highly subjective – based on the claimant's perspective. Furthermore, our mental states are precarious – Alzheimer's disease can erase an entire lifetime of memories and many attributes of identity. Amnesia can obliterate one's entire sense of self and questions around potential Cerebral Cortex transplants shine new light on the old Ship of Theseus paradox.

Social Traits

As is clear from the derivation of many last names – what role a person plays in society is an important aspect of one's identity, consider the modern business card. Like physical data, the characteristics that comprise social identity also evolve and change over time. Similarly to mental data, social data can be difficult to prove as fact.

Social data consists of the performed roles individuals act out when engaging in society – just like actors in a play. Whether we are aware of it or not many of the social roles we encounter in society are chosen by us when we assume them. For example, if Billy becomes a doctor, he alone opts to perform this role, willingly assuming the position as part of his identity. Likewise, a person often has the choice to no longer play that role.

It is in these social roles that a person's actions are witnessed or experienced by those around them and in turn shape the social identity or perception of an individual, such as Billy, in the eyes of others. Indeed, Billy's actions might be a very good indication of what sort of person he is – arguably more reliable than what he claims to be.

Awareness of social roles, such as parenthood, profession, or community participation, can lead to a sense of personal responsibility. Understanding first that we even choose roles and secondly what degree of responsibility comes along with those choices is the very essence of our existence. It is with this sense of responsibility for one's actions that can prevent a person from consciously doing harm to others, seeking to protect his or her identity inasmuch as identity is considered something akin to reputation. Ultimately, the more people who develop such a sense of responsibility the more secure a society becomes as the likelihood of misdeeds drops. Unfortunately, there seems to be an ever-greater number of individuals who fail to develop such a dual concept of opting social roles as well as the inherent responsibilities that come as a result of interacting with members of the group.

Although social roles can be unique characteristics used to identify individuals, few social roles remain the same over the course of a lifetime. Billy may begin life as a son, but he may close it as a father or a grandfather. He may also change professions several times over the course of his life. Likewise, Billy's behaviour is likely to change over time – as disposition and preferences are often altered by one's responsibilities and state of emotional or mental health. Finally, social roles like memories can be easily falsified – a person may claim that he or she has assumed certain roles in society when in fact he or she has not. The fabricated resume is perhaps the best example of this.

Physical Traits

Physical characteristics are considerably easier to distinguish and are one of the first differentiations made between individuals. People stand out as being different from one another based on their hair and eye colour, their physique or any scarring or markings they may bear. In this manner, we seek to tell the difference between one person and another – thus identifying individuals as being unique.

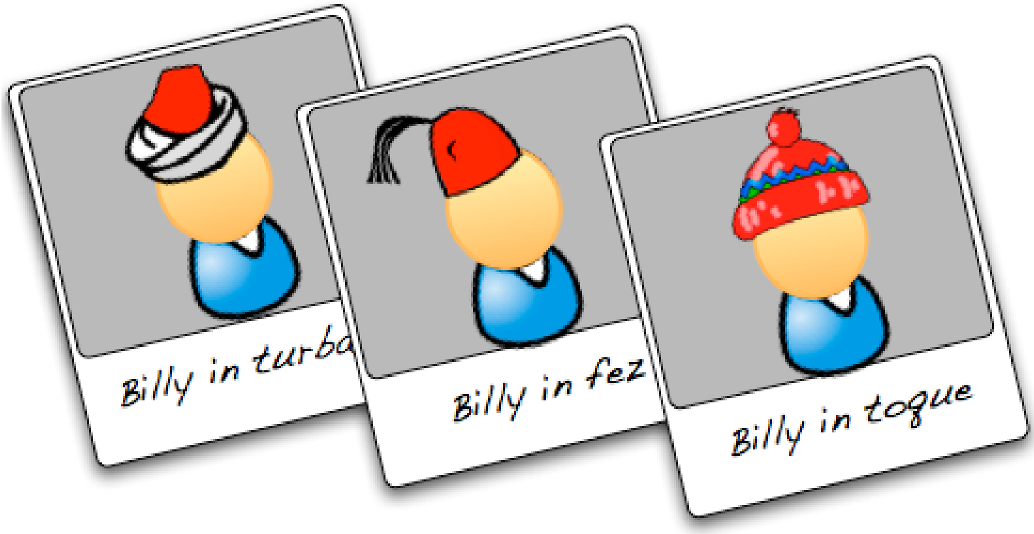
Qualitative Identity

Homo sapiens, however, are remarkably similar physically.   Cases of mistaken identity are common and easy to make – if Billy has a twin, Bobby, consider how similar the two might look. Most humans are in terms of physical appearance, qualitatively identical – that is the majority are exactly similar, having only one head, two legs, two eyes, two arms etc. Bobby and Billy are qualitatively identical. They are, however, not exactly the same as one another, or numerically identical, as they are clearly two separate beings.

Billy & Bobby
Twins - 6 years

Numerical Identity

If a person is numerically identical with someone else – it by default means that the two are, in fact, one and the same. To be numerically identical implies that something is exactly the same as another – there can be no multiples. Consider the case of Billy – regardless of how Billy alters his outward appearance through disguise he remains Billy. Billy is numerically identical with himself regardless of what he wears.



Billy in turba

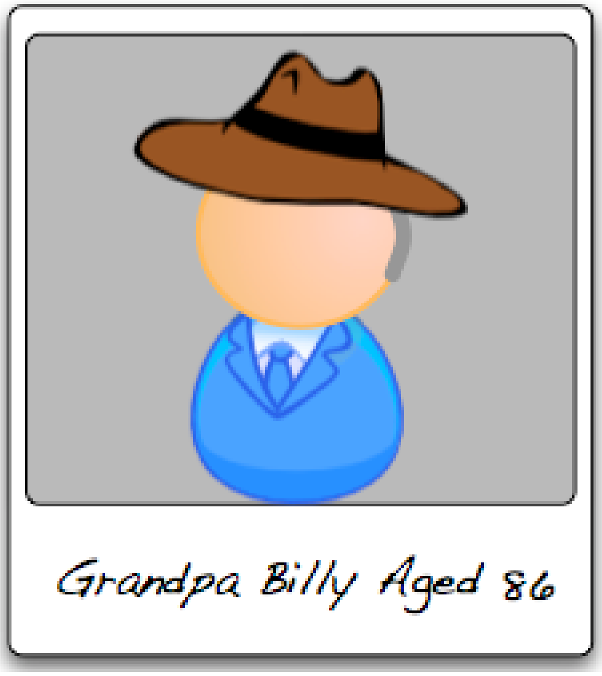
Billy in fez

Billy in toque

Identity as it is used in our system today is based on the concept of numerical identity. Although people are qualitatively identical, it is assumed that each individual holds their own numerical identity – that can be measured and persists over time. Given the overall similarities humans share – emphasis is put on ever-smaller differences that when compiled in a template-like format (eye colour, hair colour, height, race etc.) might be compared in relation to one another in order to establish a unique identity.

Biometrics

Biometric identifiers, such as finger and palm prints, iris and palm vein patterns and DNA have been steadily growing in popularity as a means of authenticating an individual's identity with his or her previously established official identity or identity template. Indeed, the unique patterns formed on the tips of Billy's finger are distinctly unique even from his twin Bobby's fingerprints, providing an effective means of verifying that Bobby isn't Billy. This can be done either by comparing the prints of both men if they are physically present or by comparing the samples presented against previously stored prints in a database. In fact, physical biometric data is perhaps the only reliable method currently available by which we can quantifiably measure a person's uniqueness with a high level of accuracy.



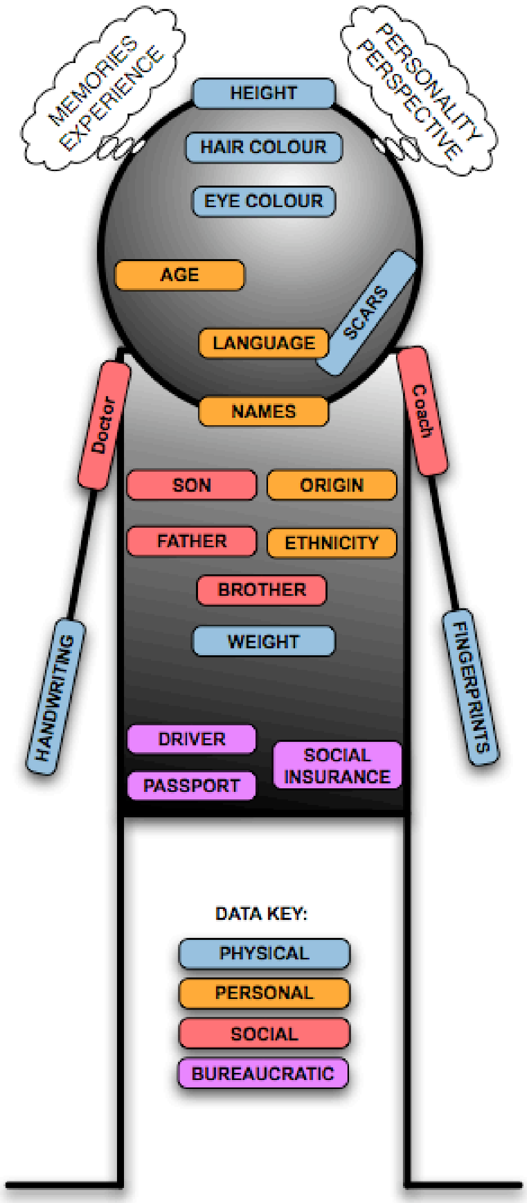
Biometric systems, however, are still subject to error – being 'spoofed' by fake gelatine fingerprints, amputated digits or contact lenses to generate false positive matches, whereby a biometric system registers a match between two prints which are not identical or to prints that are incorrectly linked to an identity, creating an ongoing challenge for biometric system developers. Yet perhaps the real danger beyond the use of biometric systems used to differentiate and authenticate the identity of individuals is the risk of becoming overly reliant on technology to solve human problems or shortcomings.

Physical attributes remain the most used form by which we compare individuals and establish uniqueness. This is quite possibly due to the ease with which these traits individuate people. Yet just as physical attributes are used to differentiate – so too can physical attributes be used to alter an identity. Hair colour can be changed in half an hour with hair dye, contact lenses can turn blue eyes to brown in seconds, weight is easily gained or lost and adding or removing facial hair has long been a favourite for masters of disguise. In extreme cases, physical attributes can be very much altered through plastic surgery. This is to say nothing of the unavoidable changes brought on by time and aging – Billy in his twilight years will be certain to look very different than he did as a child.

Who is Billy?

By the time Billy Schumacher comes of age much of his identity will have become fixed – or will it?

In terms of personal data (so long as he does not alter it in any way) his name is WIlliam Schumacher, born July 5th, 1920 to Günter and Mathilde Schumacher. Billy' is ethnically German but his nationality is Canadian as he was born in Kitchener, Ontario. Billy is bilingual, speaking German and English.   Although raised in a Lutheran household, Billy is presently an atheist.



Billy likes to tell stories about his childhood – his twin Bobby, the over eating at Oktoberfest, work on the farm and quiet Sundays. The memories he relays are very detailed. There is no reason to doubt that he hasn't lived the life he claims to have.

Physically, Billy is of average height and build. Billy has brown hair and blue eyes. There are no obvious scars or markings by which to distinguish Billy. The fingerprints he put on record last year just in case he went missing match those he has now.

Socially, Billy has been a son, a brother, a father and a grandfather. Billy has worked as a farmer and a doctor. In his community, Billy volunteered time as a coach to his son's hockey team and once ran for mayor in one of the communities in which he lived.

Yet proving that Billy Schumacher is in fact who he claims to be would still be a point of contention. If Billy were to travel out of his hometown where neighbours are no longer available to vouch for him (which still does not irrefutably prove it as fact) how could his identity be proven as authentic? How can the labels ascribed in the making of an individual be proven?

Bureaucratic Traits

To solve the problem of authenticating identity in the public realm, categories are assigned to those attributes that each of us use to build our identity. Numbers and cards are issued to individuals registered in a system to help each of us prove that our claims to our identity (and the privileges that come with it) are indeed genuine. The premise behind such a system is that only official identities would be issued corresponding documentation and as a result a person holding a card that matches his identity claim would be telling the truth. The data associated with this aspect of personal identity consists of our bureaucratic traits.

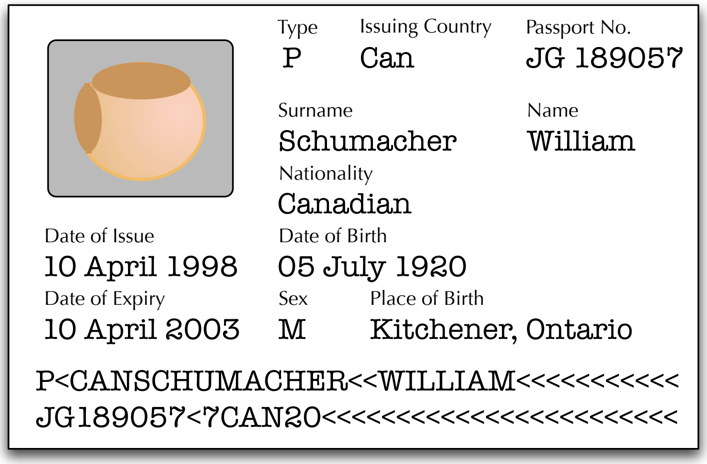
Before the industrial revolution the problem of mass identification of individuals was not the issue it is today. The average person travelled as far as their feet could carry them, which meant little beyond their immediate environs. People lived and died where they were born and most likely their parents and grandparents before them, although this remains unchanged for some, in North America moving considerable distances has become commonplace. Any details associated with a person's identity were hard to fabricate in local communities – an individual's occupation, parentage, physical appearance and actions easily differentiated them.

Authenticating an identity arose as a means to verify that one had authorization to travel or was recommended by a person of repute who knew the traveller. In this sense, identification was more closely linked to the originator of the permit or substantiation rather than the individual themselves. Indeed, our focus on what country an identity document or passport originates from today is little different. As populations boomed and ever-greater numbers of people began moving house from one country to another, emphasis on individual identity grew.

Perhaps no other events demonstrated the need to have a systematic and internationally recognizable process for authenticating individuals' identities as World Wars I and II. Although many states had been documenting information on citizens, the means for an average citizen to prove his or her identity (particularly outside of one's country of origin) was lacking. When Europe found itself in the throes of war there arose great interest in managing the travel of individuals across borders – preventing some while allowing others. Building on existing travel documents – such as letters of permission and verification papers – the modern passport was developed.

Today, barring advances in technology, the concept of an identity document remains the same. At birth – in order to verify the event in the future – a registered child is issued a birth certificate, which states his or her name, date and place of birth, issuing location and gender. Assigned also to this birth certificate are numbers associated with the certificate itself and registration – the first piece of bureaucratic data correlating to identity. Physical data is often omitted, as the individual will change a great deal throughout his or her life.

Possessing a birth certificate is necessary for acquiring a host of other identity documentation. Returning to our example of Billy – with birth certificate in hand he is now able to apply for a Canadian social insurance number, a driver's licence and a passport for travel. Many of the attributes listed in these documents remains the same as the supporting document (a birth certificate) with the addition of a photo, digital watermarks, magnetic strips and increasingly a biometric identifier.



Type
P

Issuing Country
Can

Passport No.
JG 189057

Surname
Schumacher

Name
William

Nationality
Canadian

Date of Issue
10 April 1998

Date of Birth
05 July 1920

Date of Expiry
10 April 2003

Sex
M

Place of Birth
Kitchener, Ontario

P<CANSCHUMACHER<<WILLIAM<<<<<<<<<<<
JG189057<7CAN20<<<<<<<<<<<<<<<<<<<<<<<<

This system of identification is somewhat naively based on the premise that a person possessing the initial document or what is commonly referred to as a supporting document, is in fact the original possessor of the document. Unfortunately, this is increasingly not the case.

Cases of identity fraud and theft are on the rise in many countries and organized crime and espionage rings continue to build false identities founded upon official identities held by both the living and deceased. In these instances, the identification cards held by the impostor can match their physical description including biometric prints. Unless the person inspecting the document was aware that they are confronted with an impostor, they would check the document, compare it against the holder and deem the identity legitimate. In many cases, using a document to prove that the carrier's claim to the corresponding identity is genuine is little more reliable than the memories or characteristics they purport to hold.

Nevertheless, it is around the concept of identity or who we claim to be – our names, characters, lives we lead and physical attributes – and our reliance on documentation to authenticate our claims - that we base many security measures.

Border Security

Having presented his supporting documents, submitted his application and fee for enrolment, Billy Schumacher is issued an official passport. Billy is now ready to cross all the international borders he is permitted to.

The role of identity in border security is one of managing millions of individuals that travel across international borders each day. In this sense – it is thought that by noting the movements of the masses those people who pose a threat to society can be discovered and apprehended either for crimes already committed or even better – before any crime has even occurred. The ability to distinguish individuals through their respective identities is accepted by many governments and organizations as a means to identify and thwart human threats.

A system can be quite functional for managing law abiding citizens – and even more so for those citizens residing in the same country in which they were born. However, managing the identities – the births, internal migrations and immigrations, name and physical changes and deaths – of millions of people is a gargantuan task. Errors are bound to occur – and at times stories surface of a person living successfully under an assumed identity.

The technology used – computers, databases, networks and large-scale identity management systems – are increasingly being turned to in a bid to authenticate border employees' and travellers 'identities. However, many concerns surround the security of such systems. Having transitive trust in a document or third party also entails trusting the identity management system that was designed to enrol, revoke and issue an identity document. Who would have ownership of as well as access to the database? Who decides just what information would be housed within it? This is to say nothing of the costs of implementing and maintaining such systems.

Given that identity is such a fluid concept it is not inconceivable that a person could fabricate their personal details and past history to create an identity under which they live. Although acquiring official documentation to support these claims might not be simple – it is not impossible. The means to establish an official identity under false pretences include but are not limited to: establishing an identity with documents from another country, the use of stolen passports either already issued or *en blanc,* bribing a corrupt official to issue a legitimate document under a false identity or assuming the identity of a deceased person approximately the same age as the impostor. As a result, comparing an identity document to the person holding it doesn't necessarily prove an identity authentic at all – even with a corresponding biometric print stored in a microchip on the card.

Indeed, organized crime syndicates have long had footholds into bureaucratic departments responsible for the establishment of legitimate identities and the issuance of corresponding identity documents. Corrupt officials that issue legitimate documents not only facilitate the establishment of new, fraudulent identities but also tip off organized crime counterparts when any drastic changes are made that might affect the ability to effectively use forged documents. This is not a problem that technology can solve alone – surely the use of expensive national identity document systems cannot answer it. In many cases criminals already possess and live legitimately under these falsified identities and will be issued new high-tech documentation that then matches their existing official persona. Perhaps an identity management system could decrease the likelihood of such corruption by monitoring and assessing officials who are responsible for establishing identities and issuing corresponding documentation rather than opting for the implementation of more costly national identity document enhancements and systems.

Identity, however, can be a viable measure to distinguish known targets from other travellers. A suspect who has changed little from their physical description, left behind finger or palm prints at a crime scene or is still travelling under their original name/identity can be uncovered under the current system and apprehended. Identifying and capturing individuals who have changed their appearance drastically, assumed entirely new and official identities and for whom there is no biometric evidence available, the task becomes far more difficult. Expecting identification to help pinpoint unknown threats such as would be terrorists, murderers or other criminals entering with official identity documents before a crime has even been committed, is wishful thinking.

Identity is only as useful as the information associated with it – if there is no past attached to an identity that gives rise to alarm. Why should the person claiming a certain identity be questioned or detained? As a security measure, focus on identity is reactionary – meaning that any increase to security through the use of identity occurs after the fact, after a person has committed a crime. Identity can abet officials in identifying and detaining perpetrators and hopefully prevent that known culprit from committing future crimes. That the use of identity in security is reactionary, however, makes it highly unsuitable for the prevention of crimes such as terrorism. Yet many countries have been turning to processes built around identity as a so-called preventative means. It is highly unlikely that terrorist groups – if organized enough to execute such attacks – would adopt personal identities that are already associated with criminal activity or originate from states that are seen as sponsoring terrorism or organized criminal activity.

Border security measures that focus on identity – in particular those that have been recently implemented or are proposed using advanced technologies – need to be revisited. At present, the trade-offs, risks and costs often outweigh the effectiveness of implementing a particular solution, offering little more than another reactionary measure. For example, facial recognition systems have been shown to have high error rates resulting in many false positive and false negative matches. The operational costs of errors occurring as a result of the technology, decisions made by border guards based on an over reliance of technology as well as the costs of implementing such systems suggest that many of these pending projects should be carefully re-considered.

This is not to suggest that the use of identity and associated systems should be left behind entirely. Indeed, there are few other options currently available and some systems function quite effectively if they are used for authentication rather than identification purposes. Likewise, there are a number of other ways in which border security can be more effectively improved – including some more proactive measures.

Upgrades to computers, networks and connectivity used in border security can ensure that searches against databases of known offenders or wanted individuals can be executed more efficiently and effectively. In addition regular maintenance should be carried out on these databases to ensure that all information stored within is up-to-date and accurate.

The use of ever-more sophisticated security printing techniques such as holograms or watermarks can help deter counterfeiting. Machine-readable travel documents, however, are a double-edged sword. In some border terminals, machine-readable equipment was installed to speed-up the process of crossing the border. Such crossings very often occur without any direct contact with border guards unless the system detects a problem with the actual travel document. Although the use of scanners and readers allows the authorities to reduce wait times, unless border guards are required to pay more attention to the traveller's behaviour instead of checking documents, the use of scanners could create over-reliance on the technology to authenticate identity documentation. A combination of traditional security methods visible to the naked eye as well as more technologically advanced means would be the most effective as a result.

Fostering quality border personnel can also greatly improve observation techniques and as a result border security. Increasing border patrol salaries to entice those candidates with educational backgrounds in the study of human behaviour or by offering similar training may increase the likelihood that certain behaviours can be identified more accurately. Border personnel should also be regularly rotated to avoid errors associated with monotony of task performance.

Ultimately, border security must be considered from a holistic perspective – no single measure will effectively increase security alone. Indeed, the prevailing focus on identity and identity documents in border security measures appears to be an attempt to create the sense that security has been increased when in fact it has not.

Perimeter Security

Although the use of identity in perimeter security is similar to border security – in the sense that it is used to allow pre-approved individuals access to a restricted facility or area – the use of identity tends to be more effective within the perimeter security model. The focus on identity in perimeter security is one of verification whereby those attempting to gain access to the area are searched against preauthorized individuals with the authority to enter.

In securing a facility or closed area collecting information about a person's identity can be an efficient means to ensure only those people authorized can enter. In such a system the number of authorized individuals is finite – and those persons are known beforehand, already having undergone a background check so they can be stored in the system.

Once Billy's identity has been accepted as authentic and acceptable to those securing the perimeters, Billy would most likely be assigned another bureaucratic identification number and possibly an access card associated with his identity. To enter the facility Billy might have to present an access card. Information stored on that access card will be searched against the database to verify whether Billy has in fact been given authorization to enter. Billy could also be asked to present a biometric identifier or a password to further verify his identity as an authorized individual.

As with all areas of security - nothing is certain. A person of similar description to the authorized individual with the know-how to fool biometric systems, create copies of access cards or acquire secondary authenticators such as passwords can still breach such a system. This is to say nothing of a physical break-in or the forced entry of the perimeter with the help of an authorized individual. The official identity of a person authorized to access the facilities might have been fraudulent – and thus all other identities based on the original official identity are then questionable and constitute a breach.

Yet, beyond this, perhaps the most troubling aspect of the use of identity in all security is the inability to truly be certain of a person's intentions. Authorized individuals can easily become double agents or disgruntled employees. Absolute proof that a person is or will remain, in fact, who they claim to be is impossible – such is the nature of the many characteristics comprising identity. At a time when more and more attacks on organizations are being traced back to insiders, other means to monitor and assess those with access need pursuing. As mentioned, the use of identity can be helpful in pointing out a perpetrator – but it certainly cannot prevent an attack. Indeed, understanding and monitoring human behaviour or changes in mental states of those with access would offer a great deal more in terms of prevention.

To increase the effectiveness of perimeter security based on identity, automatic entrance points should always be manned by a guard as well as monitored through surveillance cameras. Although not foolproof, gaining entrance into a secure area can be made more difficult by requiring the usual access card as well as secondary authenticating information such as unique key codes or a biometric identifier. Again, databases that store and manage identifiable information should be kept up-to-date, ensuring for instance that stale accounts are no longer being used to gain access past the perimeter.

Corporate Identity Management Systems

If Billy were to apply for a job in a modern organization he might find himself with yet another identity in order to interact with the environment around him. The use of identity to enhance security measures within corporate computer networks can also be effective. Similar to the perimeter security model, an organization will commonly know in advance with whom it is engaged and whether they are employees, partners or clients.

Information about identity stored within corporate identity management systems, is based on existing information relating to an individual (names, address, date of birth, social insurance number etc.) as well as the individual's role within the organization. The individual is then assigned a 'virtual identity' that allows for access to different tools and resources within the corporate network, depending on their role and responsibilities. Typically, passwords are used to ensure that unauthorized access is not granted through the use of a registered user account. However, passwords are increasingly becoming a potential security breach as users continue to write them down on notes left next to computers or share passwords with co-workers that might not otherwise have such access privileges. As a result, the use of biometrics is proving a popular alternative to passwords.

Identity management systems have been steadily gaining in popularity as a solution to comply with laws such as Sarbanes-Oxley. Indeed, such a system offers the ability to accurately track who has had access to which areas of a network, what has been done to any data and when it occurred. As with the example of perimeter security, the system is also very effective in identifying the perpetrator after the fact.

However, identity management systems do little in preventing the growing problem of attacks made by disgruntled insiders.   Once again, it is not so much identity that should be the focus of preventative security measures but behavioural patterns. Understanding the effects of stress on workers - such as the impact on morale and loyalty as a result of layoffs or identifying at-risk employees prone to a sense of unfairness when over looked for promotion or a raise – can act as the first buffer against potential attacks.

The efficiency of corporate identity management systems can be increased, like those used in border and perimeter security, through the regular maintenance of accounts – including the revocation of access or deletion of old accounts. Along with regular inspection of existing accounts to ensure stale accounts are deleted and access to existing ‘virtual identities’ corresponds to the role associated with the corresponding individuals. Failure to manage accounts and keep the system updated renders a corporate identity management system useless.

Conclusion

At a time when the biggest perceived threat to many states’ national security are unknown entities operating in distributed terrorist networks, the question begs – why are we continuing to focus so much on identity as a security measure?

Identity is an ever-changing set of characteristics we associate with ourselves in an attempt at individuation. Although we all possess some form of identity the ability to authenticate that identity to an irrefutable degree of certainty is nonexistent. Despite the best bureaucratic efforts to establish some means of verification – the issuing of cards is no more reliable than what a claimant insists their identity to be. The ease by which fraudulent identities can be officially established all suggest that identity at the very best offers a reactionary means to potentially weed out known culprits or identify perpetrators after a breach.

Implementing costly technological solutions to revamp a system that is innately problematic – as a result of the inconclusive nature of identity – needs to be considered from an angle that takes the actual concept of identity into consideration first, both as a separate concept and as part of a larger consideration of ‘What is Security?’ Indeed, identity-based solutions in border security measures can at best offer a reactionary increase to security. This suggests that the costs and implications of using these systems can outweigh the risks associated with the breach itself.

Used in solutions where finite, previously identified individuals are being granted access to physical or digital perimeters is perhaps the most efficient application of identity in a security measure. Despite such a system’s ability to at least identify most of the users entering into the secured area, however, it does not prevent inside attacks or determine which individuals might be operating under fraudulent official identities. The likelihood of at least pinpointing who perpetrated the attack is afforded in such systems – but again is only as valuable as the accuracy of the information provided by that individual beforehand. Background checks are important. Yet perhaps of even more importance is the development and employment of an understanding of behavioural analysis and profiling to detect changes in at-risk employee behaviour.

Without first considering the inherent flaws of limitless security systems based on identity, governments run the risk of being caught in a vicious circle. The costs of such national identity programs are immense. The technology needed to implement these systems is substantial and often cutting edge. However, spending billions of dollars to enhance an innately flawed system already infiltrated by organized crime syndicates and open to so many other possible breaches is worrisome. Using technology as a means to try and fix a defective system opens a proverbial Pandora's box. As breaches arise from social engineering scams or news surfaces of criminals continuing to successfully acquire and live under legitimate yet false identities, faith in the system will diminish. Coupled with continued pressure from privacy advocates the public will increasingly view these systems with cynicism and suspicion. The government will find itself with little choice but to continue to dump more money into the system. Making attempts to achieve the preventative results it had promised, again with little result in the face of growing public mistrust and dissatisfaction will only result in a full system failure. The alienation of law-abiding citizens might also drive some to seek alternatives perhaps even illicit in nature as a result of pressures and inconveniences experienced through the use of malfunctioning systems.

Perhaps the biggest loser of all will be technology. Despite what technology offers in terms of facilitation of solid security measures, its ineffective and costly application to improve a fundamentally flawed system will create public weariness towards any future advancement. If governments and technology developers want to avoid this result, proper consideration for the existing flaws of a system and the long-term implications of a project must occur before implementation.

Nothing can solve human problems but humans. Security measures should be created by first considering the human element or those human reactions to an event that can further destabilize the state of security post-breach. In this sense, it is the person – not individual attributes or the technology – that is the underlying risk and must be considered above all else before a reasonable security measure can ever be formulated.

From a holistic perspective, security measures involving identity are not the only measures needing reconsideration. Often our focus on what might breach security blinds us from concurrently studying what might strengthen it. As a result, no one solution or focus can be said to effectively increase security on its own. As it stands, our Billy Schumacher is no less real than others, but relying on identity to determine this is currently flawed.

Further Interest

Campbell, David, “National Deconstruction: Violence, Identity & Justice in Bosnia”, University of Minnesota Press, 1998

Castells, Manuel, “The Power Of Identity”, Vol. 2, Blackwell Publishers, 1997

Costner Sizemore, Chris, “Mind of My Own: The Woman Who Was Known As “Eve” Tells The Story Of Her Triumph Over Multiple Personality Disorder”, William Morrow & Co, 1989.

Locke, John, “An Essay Concerning Human Understanding”, Hackett Publishing Co. Inc., 1690

Schneier, Bruce, “Beyond Fear: Thinking Sensibly About Security In An Uncertain World”, Copernicus Books, 2003

Taylor, Charles, “Source of the Self: The Making of the Modern Identity”, Harvard University Press; Reprint Edition, 1992