People, Policy and Technology: Considerations in Designing a Robust Security Framework

Michael Reed
Systems and Communications Executive
PB Australia-Pacific
GPO Box 5394
Sydney NSW 2001
AUSTRALIA
mreed@pb.com.au
+61 409 298 208

Abstract. This paper analyses the process which was employed in defining the security architecture for a latest-generation Electronic Toll Collection (ETC) system. It focuses on one fundamental operational requirement – the non-repudiation of transactional data and the evidence of travel in support of the enforcement of tolling events – and uses this to highlight the essential integration between technological capability and operational processes in delivering a secure solution.

Put simply: in a market of off-the-shelf security "solutions", it is essential at the enterprise level to recognise that security is a process, not a product.

The interactions between technical and technological capabilities, operational policies, people and business processes must be tightly aligned in order to demonstrate that the enterprise has achieved the non-repudiation of transactional data, and has a sound basis for tolling.

INTRODUCTION

Implementation of a robust security architecture has become a pre-requisite for technology-based enterprises. Across many industries and jurisdictions, detailed and onerous regulations exist to define minimal levels of security application. These regulations are commonly focussed on ensuring data privacy. The rapid growth of business-to-business services has exponentially increased the points of ingress to corporate systems, and hence the number of gates that 'need to be patrolled'. Being a high-technology industry, ETC concessions need to ensure that they are complying with the appropriate security regulations and privacy legislation in the implementation of their underlying systems.

Additionally, in a multi-lane free-flow environment ETC transactions must be based on remote and reliable identification. Whether this is achieved through unique transponder (or 'tag') detection, or identification based on capture of licence plate images, once the vehicle has left the tolling point, the data captured (often at highway speeds) will represent the only evidence that will ever be available to substantiate the passage. Consequently, in addition to guaranteeing the standard requirements that data has been protected, the nature of ETC

further necessitates non-repudiation of transaction data in order to support a toll charge or provide evidence for enforcement.

THE PROJECT

EastLink is the largest urban road project to date in the Australian state of Victoria, with a construction cost in the order of AUD2.5 billion. The project is Victoria's second multi-lane free-flow electronic tollway, the 39km motorway linking the Eastern Freeway with the Frankston Freeway in Melbourne's south-eastern suburbs. EastLink will deliver more than AUD10 billion (Allen Consulting, 2006) of direct benefits to the state of Victoria over the life of the project.

In October 2004, ConnectEast was awarded the contract to fund, design, build, own and operate EastLink for a period of 39 years.

Described in Systems Engineering concepts, the EastLink Electronic Toll Collection (ETC) system is a System-of-Systems. It delivers a variety of large-scale inter-disciplinary business solutions through implementation and integration of multiple heterogeneous, distributed systems that are embedded in networks at multiple levels and in multiple domains.

The Project Legislation, Concession Deed and Contractual framework for delivery of the Tolling System considers non-repudiation at a number of these levels. This report will outline the process by which the Tolling System and Tolling Operations Analysis has been performed with respect to satisfaction of non-repudiation and objectively demonstrate satisfaction of the Requirements.

In order to satisfy the requirements for prosecuting the offence of driving on EastLink without payment of toll as defined above, the concessionaire will be required to certify statements as defined in the Project Legislation (EastLink Project Act, 2004). The two fundamentals upon which this certification is based are:

- That the vehicle was driven on EastLink
- That the toll (and/or toll administration fees) has not been paid

The ISO standard covering IT security techniques (ISO 13888-1:2004) identifies "the goal of the non-repudiation is to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action".

In this context, the primary objective of the non-repudiation service within the Tolling System delivery is to demonstrate the validity of evidence presented in support of claimed and unpaid travel on EastLink. This is the service considered in this report.

BROADER SECURITY CONTEXT

Non-repudiation of an underlying commercial transaction is only one component of the overall security obligation modern enterprise must address in operation.

In today's economic, political, and social environment, addressing security is becoming a core requirement for organisations. Customers are demanding it as concerns about privacy

and identity theft rise. Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. National and international regulations are calling for organisations to demonstrate due care with respect to security and privacy.

Enterprise must consider the potential cost implications if, for example:

- customer data is compromised, and the implications of public knowledge of such an infringement
- your brand and reputation are negatively affected by a security breach, resulting in a loss of investor and consumer confidence and loyalty with potential commercial ramifications related to the financial stability of the organisation
- sensitive intellectual property (such as trade secrets and new product information) is stolen by a competitor or made public
- your organisation is found to be non-compliant with regulations (national, state, local) as they relate to the protection of information and information security
- your network goes down because of a security breach
- the organisation can not detect a security breach

The realistic frequency of these security incidents have been assessed through recent economy-wide surveys (Richardson, 2008), which indicated:

- 46% of respondents had experienced a significant security incident within the previous 12 months
- Insider abuse of network access increased from previous surveys to 59% as measured across types of “attacks” detected in the previous 12 months
- In response to a reported incident, 34% of organisations changed their organisational security policies

The lynch-pin of an enterprises security framework has been in many cases the advanced and highly-configurable security technologies implemented. However this survey reflects the significant part played by human resources in both effecting security breaches (reflected as “insider abuse”) and protecting against them (through robust security policies, processes and procedures).

Rather than solely wrap the enterprise in a layer of technology based security applications and components, the current view of Enterprise Security Architecture reflects the PPT methodology.

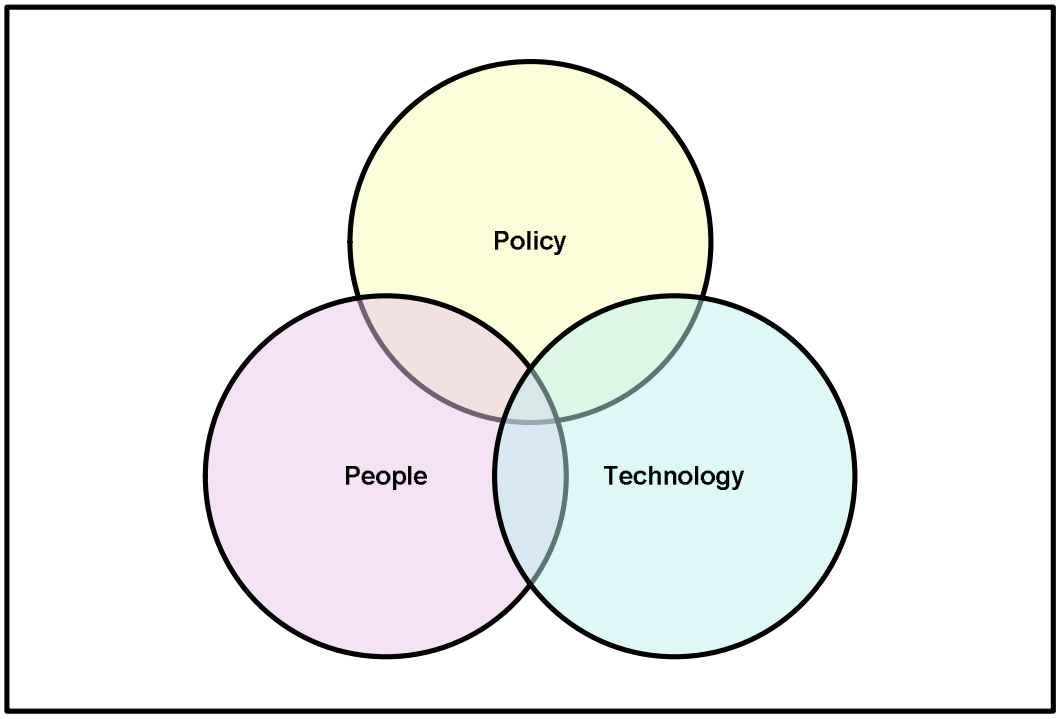

Figure 1 Security Framework: People, Policy and Technology

PPT stands for People, Policy, and Technology. The security process is a mixture of these three elements. Each element depends in some manner on the other elements. Also, issues receive greater coverage when the elements are combined. The controls environment is greatly enhanced when these three elements work in concert. A simple drawing (Figure 1) will suffice to illustrate this. This drawing shows the basic elements and also the coverage areas.

ENTERPRISE SECURITY ARCHITECTURE

Enterprise Security Architecture is the application of a comprehensive and rigorous method for describing procedural structure and behaviour for an organisation's security processes, information security systems, personnel and organisational sub-units, so that they align with the organisation's core goals and strategic direction. Although often associated strictly with information security technology, implementation requires direct alignment more broadly to the security practice of business optimisation in that it addresses business security architecture, performance management and security process architecture as well.

As a direct result of the increasing focus on security and privacy, Enterprise Security Architecture is becoming a key objective of enterprise system delivery. The primary purpose of creating enterprise information security architecture is to ensure that business strategy and Information Technology (IT) security are aligned. As such, enterprise information security architecture allows traceability from the business strategy down to the underlying technology.

CORPORATE GOVERNANCE AND SECURITY

Research at Carnegie Mellon University's Software Engineering Institute (Julie Allen, 2005) has identified the following set of beliefs, behaviours, capabilities, and actions that consistently indicate that an organisation is addressing security as a governance concern:

- Security is enacted at an enterprise level. Organisational leaders understand their accountability and responsibility with respect to security for the organisation, for their stakeholders, and for the communities they serve including the Internet community, and for the protection of critical national infrastructures.

- Security is treated the same as any other business requirement. It is considered a cost of doing business, not a discretionary or negotiable budget-line item that needs to be regularly defended. Business units and staff don't get to decide unilaterally how much security they want. Adequate and sustained funding and allocation of security resources are required as part of the operational projects and processes they support.

- Security is considered during normal strategic and operational planning cycles. Security has achievable, measurable objectives that directly align with enterprise objectives. Determining how much security is enough equates to how much risk and how much exposure an organisation can tolerate.

- All function and business unit leaders within the organisation understand how security serves as a business enabler (versus an inhibitor). They view security as part of their responsibility and understand that their performance with respect to security is measured as part of their overall performance.

- Security is integrated into enterprise functions and processes. These include risk management, human resources (hiring, firing), audit/compliance, disaster recovery, business continuity, asset management, change control, and IT operations. Security is actively considered as part of new-project initiation and ongoing project management, and during all phases of any software-development life cycle (applications and operations).

- All personnel who have access to enterprise networks understand their individual responsibilities with respect to protecting and preserving the organisation's security condition. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

These beliefs, behaviours, capabilities, and actions are reflected in a shift in perspective, with regards to the role of security within the enterprise:

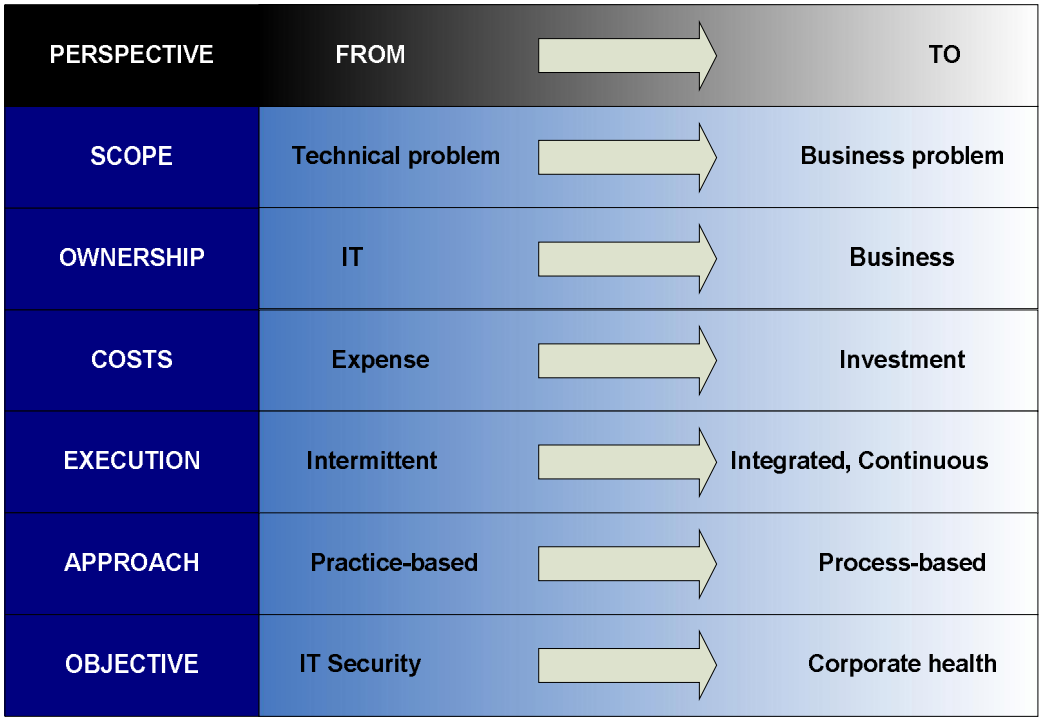

Figure 2 Security Framework: People, Policy and Technology

Because of its potential impact to business reputation, trust relationships, competitive advantage, and the confidence of investors and trading partners, information security is no longer the sole province of the IT Department. Security is a business operation that must be run like a business operation.

BARRIERS

Attending to security at the enterprise level is often hard to justify. For those responsible for security, it is often difficult to persuade senior executives and boards of the need to implement enterprise security in a systemic way. For most organisations and for most people, security is an abstract concept, concerned with hypothetical events that may never occur. Security cannot be contained or delegated to a specific function or department within an organisation.

Although many have treated it as such, missing constituent elements of people and process, security is not just a technical problem. Many functions and departments within the organisation need to interact to create and sustain an effective security solution that includes technological, organisational, regulatory, economic, and social aspects.

Security is sometimes described as an emergent property of both networks and the organisations they support. What this means is that the precise location where security is enacted cannot be identified, as its condition is often reflected in the intersections and interactions of people, process, and technology. As the organisation and the underlying network infrastructure change in response to the changing risk environment within which each exists, so will the security state. Effective security can be thought of as an attribute or characteristic of an organisation. It becomes evident when everyone gets involved; creating a culture of security that displaces ignorance and apathy.

In short, security is hard to define and implement. An effective approach to governing for enterprise security must confront these barriers head on, offering counterpoints and benefits to anticipate and offset each barrier. Increasing the awareness, knowledge, and understanding of security in an organisation is a necessary first step to changing common beliefs.

PROJECT APPROACH

The ability to demonstrate non-repudiation of evidence presented in support of claimed and unpaid travel on EastLink is not possible solely through the design and delivery of technology solutions. Neither is non-repudiation an isolated activity in the business model. The systems must be considered as part of a whole-of-business security framework that incorporates not only the technology components and messaging protocols, but also the physical infrastructure (structural and technical) and the policies and procedures governing the behaviour of Operations and Maintenance staff involved.

In ensuring that the entire scope of security services are considered and implemented to the correct level, ConnectEast (CE) have based their Enterprise Security Architecture on an extension to the Open Systems Interconnection (OSI) Model.

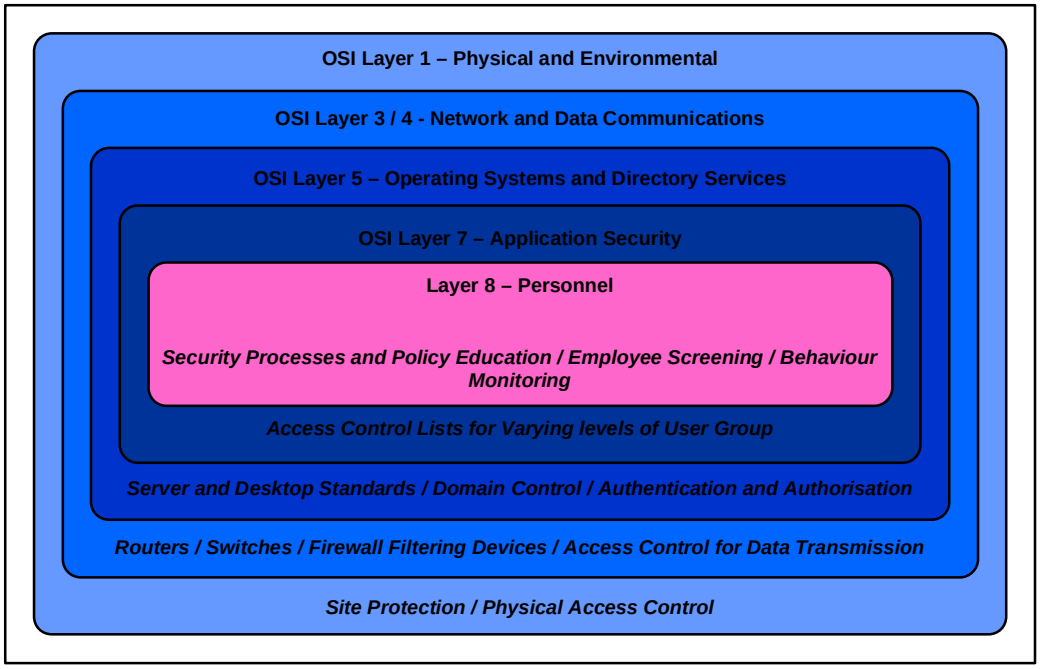

Figure 3 Security Stack

The Open Systems Interconnection Basic Reference Model (ISO 7498:1984) is a layered, abstract description for communications and computer network protocol design. From top to bottom, the standard 7-layer OSI Model consists of the Application, Presentation, Session, Transport, Network, Data Link, and Physical layers. A layer is a collection of related functions that provides services to the layer above it and receives service from the layer below it.

The conceptual addition to this conceptual view of the security stack was the addition of an eighth layer representing the impact of policy, process and procedure in the delivery of a robust Enterprise Security Architecture.

With this framework in mind, CE has based their security standards and policies on the recognised standard with relation to Information and Data Systems (ISO 17799, 2005). The CE Privacy Policy (ConnectEast, 2008), CE Information Security Standards and CE Information Security Policy consider and define security outcomes and processes across the complete scope:

- For various sites with distinct requirements (gantries, technical shelters, data centres)
- For each site, ensuring the security scope is covered (site security, physical access, cabling and network points, communication and operations management, remote access, connectivity)
- For each defined role in the Operation, policies to ensure security and access is preserved and maintained (including accompanied visits, screening, security checks)

PROJECT COVERAGE

In complying with the identified security standard, and approaching the Enterprise Security Architecture as outlined above, there were numerous regulatory and legislative requirements that needed to be incorporated within the PPT methodology. These include, for example:

- Non-repudiation of travel on the motorway, in satisfaction of the project legislation (EastLink Project Act, 2004)
- Security retention of payment card information, as defined in the industry standard (Payment Card Industry Security Standards Council, 2006)
- Compliance with the Commonwealth Privacy legislation as reflected in the (Privacy Act, 1988) and published National Privacy Principles (2008)

These (and other) security requirements were verified and validated from a number of perspectives: access controls, security systems, data security, application transaction management, and key management.

At each of these levels, the technical implementation was aligned directly with the policy, process and procedures applicable to the operations staff.

Access controls cover the domains:

- Physical security – securing authenticated and authorised access to physical sites including operations offices, server and technology rooms, technical shelters, cabinets, and gantry structures housing the roadside tolling equipment
- Network security – through zoning, perimeter security, and machine level authorisation

- User authentication – through user/role/group access to specific functionality, audit trails and access monitoring.

Security systems required design and delivery of:

- Server hardening
- Operating system hardening
- Database security and data level audit capability
- Application security and functional level audit capability

Data security incorporated virtual disk presentation dependant upon specified access control list management, and integrated technology and procedural solutions to off-line data management.

Application transaction management involved two significant domains of implementation and operation:

- Data authenticity – key based authentication of the source of tolling data between each component of the ETC system
- Data traceability – using authentication, secure keys, and, fine-grained audit capability to ensure that if the data had been in anyway altered, this was verified during the certification process (ensuring that corrupt or altered data was never used as the basis of an enforcement action)

CONCLUSIONS

An organisation must design and implement a security management process that ensures continual movement from the current state to the future state. The future state will generally be a combination of one or more:

- Closing gaps that are present between the current organisation strategy and the ability of the IT security dimensions to support it
- Closing gaps that are present between the desired future organisation strategy and the ability of the security dimensions to support it
- Necessary upgrades and replacements that must be made to the IT security architecture based on supplier viability, age and performance of hardware and software, capacity issues, known or anticipated regulatory requirements, and other issues not driven explicitly by the organisation's functional management.
- On a regular basis, the current state and future state are redefined to account for evolution of the architecture, changes in organisational strategy, and purely external factors such as changes in technology and customer/vendor/government requirements.

In enterprises that must comply with security regulations, the risk of compliance with security requirements cannot be delegated to technology providers. There is a required

intersection between the security applications, the staff who use and maintain them, and the policies within which they operate. Technology alone can not solve the security problem – security requirements must be specified in terms of capability, not specific configuration. This can only be correctly implemented in combination with the operational policies, processes and procedures to ensure the security objectives of the organisation are achieved.

REFERENCES

Allen Consulting Group, The (2006) *The Economic Impact of EastLink*

Allen, Julie (2005) "Governing for Enterprise Security", *Networked Systems Survivability Program*. Carnegie Mellon University

ConnectEast Pty Ltd (2008), ConnectEast Privacy Policy. *ConnectEast*, http://www.connecteast.com.au/page.aspx?code=privacy (April 25, 2008)

International Organization for Standardization, Geneva, Switzerland (1984), *ISO 7498:1984 Open Systems Interconnection – Basic Reference Model*
International Organization for Standardization, Geneva, Switzerland (2004), *ISO 13888-1:2004 IT Security Techniques – Non-Repudiation*

International Organization for Standardization, Geneva, Switzerland (2005), *ISO 17799:2005 Information Security Management*

Payment Card Industry Security Standards Council (2006), *Payment Card Industry (PCI) Data Security Standard Version 1.1*

Office of the Privacy Commissioner (2008), "National Privacy Principles", Schedule 3 of the *Privacy Act 1988 (Cth)* as amended 14 September 2006. Australian Commonwealth

Richardson, Robert (2008). "2007 CSI Computer Crime and Security Survey", *Computer Security Institute*

Victorian Parliament (2004 as amended), *EastLink Project Act 2004, Act No. 39/2004*

AFFILIATIONS

PB is one of the world's leading planning, environmental, engineering and project management firms. PB employs well over 12,000 people worldwide to work with our clients to reach their desired project and program outcomes. In Australia PB has been working on infrastructure and environmental projects for more than 40 years. A multidisciplinary team of over 2,400 professionals throughout Australia and New Zealand offers a comprehensive range of services, and provides total project delivery on projects of any scale.

EastLink was in 2008 Australia's largest road development. The project is being delivered by the private sector under the Victorian Government's Partnerships Victoria framework. At a construction cost of AUD2.5 billion, EastLink is currently the largest road project in Australia. It has become a major commuter road and a key intracity arterial route when it opened to traffic in 2008.

EastLink, formerly known as the Mitcham-Frankston Freeway, is Melbourne's second fully-electronic tollway, comprising about 39km of freeway-standard road connecting the city's eastern and south-eastern suburbs