INFRASTRUCTURE SECURITY
A New Approach to Critical Infrastructure Protection

Transport for London
Keeps the City Moving
An Interview With Phil Pavitt, TfL CIO

SEPTEMBER 2008
Critical infrastructure (CI) is perhaps the most complex application of IT, and carries the most severe consequences of a breach. A number of incidents in the past 10 years in the United States have proven that applying traditional cyber security measures to protect CI are not enough, and a new strategic approach is required to address this issue. Executives should develop a risk architecture that defines top priorities and make expenditures commensurate with the enterprise stakeholders’ value-at-risk.

The massive complexity of critical infrastructure systems yields multiple dimensions of vulnerability and high-impact consequences. What’s required is a consequence-driven method that can identify the high-impact vulnerabilities that lurk in physical and organizational systems and quantify the consequences breaches would have.

What’s at stake? For businesses, there are the severe economic consequences a security breach can incur, as well as issues around corporate reputation, brand integrity, and most importantly, public safety. For public entities, a breach of an essential asset such as the power grid would be enormous. Among the many consequences would be an erosion of consumer confidence in public utilities and the government itself.

Suffering the consequences

The composition of critical infrastructure is itself highly complex. The IT underpinnings combine traditional highly interconnected cyber elements with a plethora of external monitoring and communication systems. Much of this is easily accessible from open fields and Internet connections. Home users and hackers can gain access to the supervisory control and data acquisition (SCADA) systems that control energy distribution, transportation switching and public works valves.

The disparate and dynamically changing community of stakeholders, operators, owners, users and regulators complicates monitoring and incident response. Warnings of pending problems or actual incidents are hampered when multiple communication systems and jurisdictional procedures cannot cope. Moreover, the incident response systems are affected, particularly during the critical first three hours after an incident, where the tone is set for loss in lives, economic integrity and public confidence.

The impact has immediate consequences on the stakeholders and communities affected, and a significant residual effect on the rest of the nation. History has shown that this residual impact can be more costly in long-term economics due to user response, hasty and off-the-mark regulation, investor response and more.

For example, the Northeast (North America) Blackout of 2003 affected more than 50 million people and caused outage-related financial losses estimated at $6 billion. This incident exposed the vulnerability of the nation’s critical infrastructure and re-emphasized the need to take a new approach to protection. One lesson learned is that a high-impact event can be caused by systems interacting and hidden intersystem vulnerabilities exist that need to be addressed.

A new security paradigm

The CI paradox is that its highly connected nature is required for operating efficiency; however, its need for isolation is essential to protect the integrity of real-time control and monitoring.

The standard cyber security approach of looking inward, into the cyber system or data center, to find vulnerabilities is inadequate for understanding the complete impact of cyber breaches.

Advances in cyber security technology provide remarkable levels of data and network security, identity and access management, and safeguard basic IT operations. While this is necessary, it does not sufficiently cover beyond basic IT to sensor and control systems that make up the full cyber base of critical infrastructure. And there are very few cyber security solutions able to provide the required real-time protection, where a breach may have immediate and irreversible impact.

CI systems must be reflected in a total Enterprise Risk Architecture (ERA) that maps the environment from the ground under a data center through all subsystems and enterprise functions into a risk-based financial statement. This broad picture of the CI world can trace a potential breach from inception through impact as value-at-risk (VAR), or consequence, measured in economic, public reaction and public safety terms. The ERA provides the perspective necessary to identify interactions and interdependencies between different physical/cyber subsystems and organizational/jurisdictional entities, where most dangerous breaches lurk.

From such a broad perspective, analysis of the business case VAR and national case VAR can show where material consequence
problems exist. CI planners can use this information to develop system designs that reflect both business case and national case priorities that facilitate resource allocation strategies, which optimize decisions among four investment alternatives: risk acceptance, risk hedge/transfer, proactive protections and response systems. Setting these priorities can assure expenditures are commensurate with value-at-risk.

Risk analysis provides remedies
Whereas traditional enterprises understand their risk, IT-borne or otherwise, they may elect to treat it in a passive, deferred manner such as footnoting their balance sheet, subtracting a reserve from asset value or purchasing insurance. These are not responsible or publicly acceptable risk treatments for owners and operators of critical infrastructure. They must allocate resources up to the amount of VAR among protective remedies to lower the possibility of breach, and allocate emergency response systems to manage the damage after a breach.

CI systems must be reflected in a total Enterprise Risk Architecture (ERA) that maps the environment from the ground under a data center through all subsystems and enterprise functions into a risk-based financial statement. There are never sufficient resources to develop a system resilient to all threats. The consequence-driven, VAR analysis, based on a comprehensive Enterprise Risk Architecture, can enable resilient CI architectures that can tolerate high-impact breaches. Planners of new systems, as well as owners of existing systems, must begin with that analysis to gain sufficient insight into the real exposure they have.

Only then can they see how to isolate basic cyber functions from sensor and control functions, and see the intersystem gaps where hidden vulnerabilities exist. ERA examination also provides the guidance to see interorganizational problem areas and facilitate appropriate information and command sharing to reduce risk and strengthen both crisis and consequence management.

RON DICK is director of CSC’s Homeland Security Programs and former director of the FBI’s National Infrastructure Protection Center.
Worldwide CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia
139 Cecil Street
#06-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

About CSC
The mission of CSC is to be a global leader in providing technology enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client’s unique requirements.

For more than 45 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol “CSC.”