SECURING A U.N. CLIMATE CONVENTION

by Jenny Mangelsdorf

It could have been a scene from a Tom Clancy novel. Take representatives of 192 countries, mix strong feelings with serious economics and differing agendas, and it could have spelled disaster. It didn't.

Last year, CSC's StrikeForce team was tasked to assess both physical and IT security used for the United Nations Framework Convention on Climate Change in Denmark. The conference's goal: to reach a binding global climate agreement that would go into effect when the first commitment period under the Kyoto Protocol expires in 2012.

Some 30,000 people, including 15,000 delegates, 7,500 media members, and 7,500 nongovernment participants attended the two-week conference. In addition, protestors, 2,000 of whom were arrested, joined as uninvited guests. Conference floor space, which spread across more than 60,000 square meters, was webbed with almost 1,000 kilometers of network cabling, 5,000 network end points, public and private voice and data networks, and a core network infrastructure that rivaled a large, permanent data center.

A long legacy in security

"CSC has a long legacy of successfully handling very complex security issues," says Stephen Brennan, CSC StrikeForce regional lead in Australia. "In addition, CSC is the largest supplier of IT outsourcing to Denmark's public sector and our

Copenhagen data center is one of CSC's largest. It was a natural step to ask us for help when it became clear, early on in the process, that they needed our StrikeForce team to assess this very complex setup in a political arena with varied suppliers and participating parties."

StrikeForce began work months before the December 2009 conference, providing security assessment and testing of the entire cyber and physical environment in which the U.N. conference would take place. Risks ranged from espionage against participants to protecting privileged information and infrastructure from outside groups pushing specific, and potentially disruptive, agendas. Danish police were responsible for external security.

Complex distributed security

During the project, StrikeForce worked with numerous participants, including government staff, such as heads of state, police, and intelligence services; U.N. staff; nongovernment organizations; media; and IT suppliers. CSC worked with all participants to ensure the highest levels of security were achieved across all areas, including straddling groups that worked independently, but whose actions could have affected security in adjacent areas.

"One of the strengths of our distributed security assessments is that we could ensure that errors made in one domain did not contaminate controls in adjacent domains, which was a real possibility, especially given the complexity of this conference environment," says Brennan.

For example, if the wiring closets containing switching equipment around the conference site weren't sufficiently protected with physical security controls, it would have been easy for a malicious person to gain access to a trusted, secure network, explains Brennan.

Protecting highly sensitive data

During the conference, United Nations staff and delegates accessed voice and data, much of which would have been considered highly sensitive, via internal trusted, external untrusted, and semitrusted networks. During an event such as this, where hundreds of groups have different objectives and agendas, this segregation not only becomes more important, but infinitely more complex.

Everything from voice communications to print jobs needed to be protected from adjacent third parties. Hackers could have intercepted this traffic, says Brennan, by introducing a rogue access point masquerading as a legitimate wireless access point.

"By introducing rogue access point detection technology, it was possible to not only identify rogue access points almost instantly, but determine their physical location within the conference site," says Brennan. "Throughout the project, our findings and proposed mitigations increased the availability of key infrastructure and information systems."

Client: The Ministry of Foreign Affairs of Denmark and the United Nations Framework Convention on Climate Change

Challenge: Conflicting security objectives and technical challenges for the 15th Annual Conferences of the Parties, attended by 30,000 delegates, media representatives, and heads of state from 192 countries.

Solution: Perform a distributed security assessment of the conference environment, including testing and validating more than four gigabits per second of Internet bandwidth, 250 wireless access points, 20,000 ports, and a core network infrastructure that rivaled a large permanent data center.

Results: A reduced real world threat profile, increased availability of key infrastructure and information systems, improved visibility of security events historically and in real time, and a stronger overall security architecture and segregation between security zones.

Cyber reports and solutions

During the project, and after the conference was finished, we provided detailed assessment reports that identified security events as they happened and provided concrete solutions that would eliminate the potential for similar future events so they could be resolved before any damage occurred. CSC also provided a complete historical record of security events enabling users to fully investigate any actions or events that led to a failure of one or more of the security controls.

Each contractor and service provider supporting specific elements of the conference's infrastructure was responsible for fixing any CSC StrikeForce identified threats or weaknesses. CSC StrikeForce worked directly with each group to determine the most effective and appropriate remediation plan based on the security objectives, time, and budget.

"The most effective approach is not always to throw money at a problem," says Brennan. "In fact, not one of our findings required the purchase of any additional system or software. By focusing on the real business risks in the actual environment, we managed to have a conference without any IT security disaster." ■

JENNY MANGELSDORF is a writer for CSC's corporate office.