

2010 Winter Games

takes a

what's best approach

to

IT security

by Brian Phillips

Since dedicating my life to law enforcement, security and first response, I find serious “what if” scenarios.

But what if we changed our focus from “what if” to “what’s best,” from defence to offence?

Instead of getting caught up trying to anticipate everything that could happen to our vital assets, let’s start taking a look at what we have to protect and then harden it. New technologies and strategies can replace our old defensive position with a proactive stance that turns Internet security into an income generating business enabler.

How is that done? By focusing resources where they will do the most good. The Internet has about 100 critical nodes at its core – 13 root servers, 13 gTLD servers, 26 network access points and about 50 top e-commerce sites.

Should we be putting our efforts into protecting the 650 million computers in the world or into hardening the 100 critical computers that control everything? Deny unauthorized access to these hubs, and viruses and worms wouldn’t reach the critical mass necessary to become an epidemic.

Currently, the Internet is a venue for the best and the worst of human nature. When it comes to malware, we’ve seen a rapid evolution from script kiddies and hackers right up to social scammers and cyber criminals. In fact, cyber crime has surpassed the illegal drug trade as the #1 crime in Canada – and 70 percent of victims don’t even know they’ve been had. Canada is ranked ninth as an international cyber target, with Canadians standing a better chance of being a victim of crime online than on the street. Yet, of 62,000 public police in Canada, only 245 are fighting cyber crime while 18 million

Canadians are spending \$50 billion a year online.

Cyber security is more than just protecting against viruses and worms; it also involves managing information-related risk. This means controlling access to information, managing loss of data and security associated with IT, and supervising human information-handling processes.

To ensure no rock has been left unturned, Bell has taken a “what’s best” approach to its role as a Premier Partner and exclusive Telecommunications Partner for the Vancouver 2010 Olympic and Paralympic Winter Games. The 2010 Winter Games will be a microcosm of public safety and national security issues, hence Bell’s IT Security experts have worked intensely alongside the Vancouver Organizing Committee for the 2010 Olympic and Paralympic Winter Games (VANOC) for the past four years to build a robust and secure web site and network infrastructure that will stand up to the latest threats such as virtual intruders, equipment malfunctions, human error and natural disasters.

Given that the 2010 Winter Games will be the most mobile of any previous Olympic Games, with 15,000 users able to access the network anywhere and any time with such devices as a Smartphone and laptop, it is critical to ensure the network is properly protected. VANOC needs the Bell-designed network to remain secure and accessible throughout the entire Games. As such, Bell has paid exceptional

attention to building in redundancy, security, high availability and business continuity elements to ensure proper measures are in place to safeguard the network.



Author, Brian Phillips poses in front of Vancouver 2010 Olympic and Paralympic Games promo.

“Every word spoken and written, and every picture taken will cross the Bell network, so lots of eyes will be watching how the backbone of our infrastructure performs,” says Barry Caswell, VANOC’s director of IT Operations and Security. “We need to be 100 percent available during Games time, which is why we have paid so much attention to security. Should there be a single failure, a cut fibre or a landslide, the network can’t go down. With Bell leading the charge, we’ve created a risk management solution built around trusted people, processes and technology.”

The proliferation of anywhere/any time/any device communication infrastructures provides significant opportunities for both the general public and first responders to interact and receive information in real time, but it also comes with significant security risks that must be identified and managed.

At the 2010 Winter Games, any failure would be witnessed by billions of people around the world – in real time. Regardless of what form the challenges take, the first line of defence is also the first line of offence, and that’s a secure IP (Internet Protocol) communications infrastructure. In fact, Bell has designed an all-IP network for the 2010 Winter Games – the first of its kind in Olympic Games history. Also called the “Everything over IP Games,” athletes, volunteers, workers and spectators will be able to get everything they need over our secure digital network. For instance, all of the timing and scoring equipment provided by Omega, all of the cameras located throughout

the venues transmitting images to the world, and all of the countless resources and information provided on the vancouver2010.com portal runs over the Bell network.

At the 2010 Winter Games, security is not an optional extra or aftermarket bolt-on accessory. It is a core value, something that is built in from the start. For example, VANOC’s Bell-designed and managed firewall security solution involves three pillars – configuration, management and surveillance – and includes such components as authentication for authorized users, securing the perimeter through firewalls to prevent outside attacks, developing a business continuity plan, and ensuring all users are in tune with the security controls, policies and procedures from the get-go.

At the 2010 Winter Games, security is not an optional extra or aftermarket bolt-on accessory. It is a core value...

Further, VANOC’s biggest security concerns are potential cyber threats affecting the vancouver2010.com portal. These threats could involve a denial of service (DoS) that prevent the portal from functioning efficiently, eavesdropping (or “sniffing”) on conversations, tampering with scores and standings, and security of both voice and data. The Bell-integrated content distribution network combines 30,000 servers worldwide to ensure a fast user experience as well as a secure and robust system in the face of an attack.

Moving from “what if” to “what’s best”

Consider this information security checklist:

- Does your organization dedicate specific resources to security, such as budget, staffing and time?
- Is final responsibility for implementation of security placed at the executive level?
- Is responsibility and ownership/accountability clearly defined?
- Is there a user security policy or acceptable user manual in place that is updated regularly and distributed to every staff member?
- Are security policies implemented enterprise-wide, even along supply and partner chains?
- Is there a clearly documented policy for keeping networks, servers, and systems up to date?
- Is valuable intellectual property backed up regularly and stored securely? Can IT and security staff restore backups in a timely manner?
- How often is your system tested?

Anyone with basic software smarts and a bit of insider information can hijack assets and destroy systems from the comfort of their basement. Just like the players in the communications sector must harden their telecom hotels, other sectors have to harden their own network security – especially when it comes to software and cyber-vulnerabilities in their own infrastructure.

Security must be part of the critical infrastructure of organizations at all levels. Organizations need to develop a security

culture where attitudes and habits of security are pervasive. Security principles must guide process development, strategic thinking and execution. All internal and external touch points must be secured, updated and maintained by a workforce that is aware.

External audits are also imperative. In fact, they are prerequisites for effective security, and the only way to accurately test depth of protection. These audits must be performed at regular intervals, and plans must be put in place to mitigate risk from issues revealed by the audit.

“What’s best” security depends on active involvement and collaboration of all people. It’s the tool to implement proper strategic policies and procedures. Indeed, studies show that a solid emergency preparedness program and public safety plan yields a return on investment of 400 to 700 percent.

By adhering to IT security best practices, we will reach critical mass in the protection of our critical infrastructures and move from a defensive “what if” attitude to a proactive “what’s best” stance that ensures the profitability of our businesses while dramatically strengthening the security of our broader economy and communities. 

Brian Phillips is the Director of Public Safety for the Bell Enterprise Group. For more on Bell’s security solutions, visit <http://bell.ca/enterprise>.