
CBC TECHNOLOGY REVIEW

Issue 2 - June 2006

www.cbc.radio-canada.ca

IT SECURITY - BASIC INSURANCE TO PROTECT OUR BUSINESS

Broadcast organizations today face an increasingly complex work environment where security measures that were adequate even couple years ago no longer meet today's best practices. With business processes moving outside the corporate firewall to encompass mobile communications, both wired and wireless, data protection takes on a new level of complexity. As the mobile workforce stores more vital corporate information on portable computing devices, the risk of loss, theft, or unauthorized access, rises in magnitude. Moreover e-mail, the workhorse of corporate communication, faces new vulnerabilities.

It has been occasionally claimed that broadcasters are so radically different that the rules and practices developed from other industries and organizations do not apply in our field of work. The reality is proven wrong - as broadcasters become progressively more dependent on IT tools for making and transporting program material, schedules, control signals and metadata, the differences are vanishing. There is no good reason to believe that a virus that can disrupt a car maker's operation would not disrupt a broadcaster' operation. In fact, two major U.S. broadcasters experienced major disruptions last year arising from a virus attack.

For decades, broadcasters have interchanged programs in real time over expensive point-to-point/multipoint networks, which were deemed virtually impossible for a perpetrator to hack. This has led to the potential of risk-complacency within the broadcast community in assessing the risk of criminal attacks against such infrastructure. The introduction of highly popular, low-cost operating systems such as Windows, and Linux, coupled with low cost applications and IP networks for the creation, transport and storage of broadcast content, heralds a future of improved flexibility, and cost effectiveness. The conversion to digital platforms has enabled the movement of content as files or data streams, and faster than real time. The relatively low equipment cost and popularity of these technologies also mean that broadcast infrastructures, and the content they transport, are becoming increasingly vulnerable.

New regulations (Sarbanes-Oxley in the United States, Bill C-138 in Canada, require unprecedented accountability for the accuracy and protection of data. In this context, computer security is best viewed as an end-to-end solution and long term investment. Best-of-breed solutions ensure that data protection is central to everyday business processes. Every transaction or operation - entering data, transporting and storing - must be performed in a secure manner.

Regulations and common sense make it essential for an organization to search for the weakest security links. A critical examination of business processes at each stage can reveal security flaws. One flaw in a security strategy can be fatal to mission-critical processes.

For example , if an organization secures the data on all of the notebook computers used by its mobile workforce, but does not think to protect information on wireless handheld devices, this weak point can lead to security breaches.

The landscape of security suddenly changed from being optional or “nice-to-have” to being a mandatory requirement for every organization serious about protecting sensitive information and business processes. As organizations recognized that improved information security was an essential requirement, the demand rose for solutions that satisfied security considerations without reducing transaction speed. Security solutions fail if they make common tasks for everyday users too burdensome. Even as these measures become more prevalent in most organizations, the tools used by hackers and thieves are becoming increasingly invasive and sophisticated, and the corresponding level of expertise required by the perpetrators, less.

Complex operations that were difficult or impossible a decade ago can now be accomplished routinely as a part of a business's processes. Processor-intensive operations - encryption and decryption, advanced validation and authentication techniques, and biometric identification, no longer present an impediment to the implementation of sound security measures. Our business can capitalize on these technology improvements to create a secure foundation for the full range of operations and activities.

Given the challenge of elevated risks, strengthened security is no longer an optional consideration for running our business. Rigorous, multi-level security is an essential requirement of modern business operations. Some of these measures may not necessarily be popular, and may be perceived as cramping the style of an organization. But in reality, relatively minor inconveniences in the work flow are a small price to pay for the ability to maintain mission-critical operations on a 24/7 basis. It only takes one “patient zero” infection to take down an entire enterprise.

Raymond J. Carnovale
Vice-President and Chief Technology Officer