Securing Cable’s New Digital Terrain
By Julius Adams, Principal Media & Entertainment Markets at IFsec, LLC

The move to digital based distribution channels for cable operators is giving rise to a whole new array of phenomena, including ISP services, webcasting, interactive gaming, home shopping, interactive advertising, video and audio on demand, and digital content distribution. But this migration from the analog to the digital world brings to the fore serious concern regarding the protection of intellectual property – the core asset for most media and entertainment companies. The simple model of e-mail as a means to communicate more efficiently and enhance business operations has, through virus attacks such as “The Love Bug”, proven to be highly vulnerable and attacks have been proven capable of shutting down entire businesses and threatening digitized assets. The Napster controversy and the online theft of Stephen King’s Riding the Bullet also illustrate the reality of asset protection. These problems are exacerbated by the fact that security in the New Media World is very different from that in its “Old Media” predecessor.

Cable Operators are in the midst of a transformation that is demanding attention to digital content creation and delivery and connection to integrated homes through myriad end-user devices – digital TVs, digital radios, PCs, palm tops, cellular phones. These companies will be relying more heavily on alternate digital delivery mechanisms, including shared or owned ISPs, satellite, fiber-optic cable attached to cable modems and set top boxes, and microwave transmission all supported by large scale server farms.

Today’s cable networks provide ample opportunity for access to content and data through cable modems, set-top boxes, coaxial and fiber-optic cabling, amplifiers, nodes, headend gateways, and the originating internet protocol and local networks. Further opportunities for compromising streams are available through satellite links to regional headends, service distribution hubs, and digital storage servers at telephony and cable companies, production studios and interactive multimedia services.

Security Concerns Abound

System security has, in the past, concentrated on data access control and intrusion prevention that could lead to physical destruction of equipment. But the growth in Denial of Service (DoS) episodes has revealed an insidious type of attack that can halt business using high-bandwidth delivery mechanisms.

DoS attacks are an example of the problems media companies face through exposure of their systems to outsiders. Increased bandwidth is a lure to those wanting to wreak havoc with DoS attacks, system infiltration or content theft. Yahoo, considered a leader in IT methods and infrastructure design, experienced a major service outage, as did eBay and other high profile Internet sites. Yahoo service was halted by the infusion of more than 1 gigabyte per second in page requests. It would require over 300,000 users with 56K modems to send that amount of data. But with cable modems or digital subscriber lines (DSL), which are always on, it would require less than 1,000 users to achieve the same results.

Equally alarming will be the availability of content and customer data stored in digitized format at cable operator sites. Digital businesses will grow through the ability to achieve increased response to customer demands and delivery of unique content. Access to these core assets will be enhanced by the use of Internet technology for content distribution and conversely for retrieval of customer preferences and data. But with ease of access will come threats from internal and external sources. The attack on CD Universe and the relative ease with which a hacker obtained credit card information for public release and literally held a company hostage for a few days is alarming. These kind of very public incidents do not engender trust with core audiences. Cable operators intending to collect customer data will need to be aware of privacy regulations being enacted, such as COPPA designed to protect the privacy of children using interactive digital services. Responses to these regulations and the mechanisms put in place to ensure compliance will be crucial to maintaining brand image and trust.

Hacking and data theft onsite are also of concern as the value of digitized content and data becomes widely known. Employees working with external culprits, or alone, can gain access to bits of information that will...
provide access to system applications where content and data are stored. Savvy systems employees can build capabilities into systems that provide them a “back door” into protected system areas unbeknownst to management.

Crucial components of strategic systems are at risk of being compromised. E-mail carrying important strategic information and contract data, customer data, digitized content and intellectual property, web pages, and digital delivery streams delivering content are all open to misuse if not secured.

Cable modems offer a particularly vulnerable point of entry to content and data by system hackers. These modems are left on in 24 by 7 mode, and cable operators are limited in the number IP addresses they can provide, while most provide a static address. Random scanning by hackers can provide easy access to data and content traversing broadband lines connected to a cable modem. Although a firewall can prevent most attacks, hackers are finding it increasingly easier to thwart these mechanisms. Firewalls are of no use if the hacker is another subscriber to cable services and therefore already conducting scans from within the firewall protection provided by the cable operator. Data traveling through cable modems into cable lines can be read by anyone connected to the same local hub, which in effect creates a local area network of users residing and operating PCs or digital televisions connected to set-top boxes in the same neighborhood. Data and content becomes easily and widely available to anyone in the “neighborhood”.

Related to ease of access in a cable neighborhood is the ability of external hackers to enter weakly secured systems and, within a matter of seconds, utilize the system resources from which to launch attacks on other sites in complete anonymity. Cable operators whose systems are so compromised can be perceived as unwilling participants in Web attacks, causing legal and economic consequences.

**IT Security Management**

Security concerns serve to underscore the need for internal system controls and security capabilities. Enterprise-wide policies and procedures written to protect new digital businesses without hampering growth, system access control, vigilant system monitoring, and implementation of security software functionality are essential to minimizing risk. IT and business management need to work together to ensure decisions are made that enhance both asset security and business growth.

The cost of increased IT security and protection of content and data assets needs to be balanced with the investments made in front-end value added services designed for end-users. What is important to protect, and the ramifications of not protecting it, are essential questions to be answered. The increased risk of loss due to decreased brand image or trust needs to be weighed into the system infrastructure investment equation.

Risk needs to be quantified in order to develop a properly secured infrastructure and mitigate exposure. System assessments, security software selection and implementation, and event monitoring are becoming essential ingredients in the establishment and ongoing success of digital business.

Information technology units within cable operator companies will need to play a much larger role in the new digital universe than previously held by these units. IT has traditionally been seen as the provider of services for system development and “band-aiding” of applications in use by back-office functions. But the need to grow digital businesses has begun moving CIOs and their IT departments into the limelight as crucial players to the success of the enterprise through development of secure infrastructures, determining security policies and maintaining the integrity of systems.

**What Can Be Done?**

In order to know the extent to which a cable operator needs to go to secure its assets, it is important for that company to first know where it is in its digital development. There are four overall stages of digital growth that can be identified, and each of these stages brings with it a larger suite of tasks that should be considered if the company is serious about securing its content and data, and ultimately its reputation in the end-user market.
Stage 1 – Its business as usual. Cable operators are sending single-stream analog signals, and there is virtually no access to those content streams from the outside world. It is at this stage that cable operators are beginning to deal with the effects of fragmented markets, limited growth, and competition from Internet web outlets. Cable Operators are considering and developing digital strategies in order to compete, grow their businesses, and increase brand awareness.

This is a good time to consider undertaking a system security assessment and network architecture review concurrent with digital strategy planning to uncover holes in the current security configuration and determine the future state configuration that may need to be considered for digital businesses and processes.

Stage 2 – Cable operators are beginning the transition to a digital environment and realizing some success, albeit small. Digital cable plants are slowly rolling out, satellite television content distribution is maturing while traditional broadcasting is realizing steady ratings decline. Consumers are beginning to put pressure on distributors by “burning” content onto their own customized CDs. Cable operators are maturing their business plans for digital services through set-top boxes and cable modems.

At this point, it is incumbent on a cable operator to assess the current capabilities of systems to protect content and business data and to have designed a secure network infrastructure for implementation as the digital business expands. It is also important to begin considering what it is important to secure – content, data, transactions, etc. – and the potential effects on the business of not securing. Management plays a critical role in identifying the critical components of the business and determining the need for security relative to brand and speed to market.

Stage 3 – Digitization is beginning to impact the business. Broadcast television is continuing its ratings decline as cable rolls out digital delivery of programming and web products aggressively. The web begins its transition into a viable medium for content acquisition and transactions. Cable operators begin to realize success in new digital content and interactive services that connect cable customers to operator sites. Privacy, as well as content and data security, issues become prevalent as more users connect to cable operator services.

The array of tasks to be performed begins to grow and becomes more urgent to ensure content and proprietary data security, and some companies may consider outsourcing to manager services. Projects involving system security assessment and network security design need to be augmented with projects in information asset protection and security policy development. The role of privacy regulations needs to be included in decisions involving protection of data and maintenance of trust. Managed services for security administration and intrusion detection could be considered to provide ongoing protection of critical assets as the digital environment and businesses grow.

Stage 4 – Business is now operating in two modes – traditional and digital, although some may transfer to pure digital over a relatively short time. Terrestrial broadcast becomes publicly sponsored and reaches less affluent viewers as digital content distribution reaches middle and upper income homes. Consolidation will create a handful of powerful content aggregators using multiple distribution mechanisms, and distribution will reach near-100% levels. Cable, satellite and Internet reach parity levels as the TV web is realized.

At this point, cable operators should have performed a vast array of tasks that help to ensure content, data and transaction security capabilities are actively in place. Brand image and consumer trust rely heavily on providing a secure environment and addressing privacy concerns, while maintaining the ability to conduct business in an efficient manner in a competitive arena. Stage 4 companies should have performed or should be planning to perform services related to System Security Assessment, Network Security Design, Information Asset Protection, Security Policy Development, Penetration Testing and Public Key Infrastructure. Managed services for Security Administration, Intrusion Detection, Penetration Testing and Emergency Response could be
alternatives to consider for ongoing maintenance of business operations. In addition, regular monitoring of Privacy regulations and issues will enhance the ability to respond to the concerns of consumers.

By starting early, cable operators can begin to address security and privacy concerns before functional infrastructures are in place. While not impossible, the ability to successfully secure an infrastructure already in place and in use is more difficult, costly and time consuming. Without IT department and company management involvement in all areas of digital business, including security, the risks to cable operator brands are just too great.

Julius Adams is Principal of the Media & Entertainment Security Consulting practice at Ifsec, LLC. Ifsec, a New York City based company, is a recognized leader among Fortune 500 companies in developing and monitoring system and information security. IFsec has been prominently mentioned in top newspapers and business publications such as The New York Times, Los Angeles Times and The Industry Standard along with segments on CNN and CNBC responding to issues regarding data security and privacy.

Notes
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________