

A Solid Defense

As communications companies face up to ongoing erosion in returns from their traditional business, they find themselves at a crossroads. For many, the way forward lies in charting a new strategic course as multiproduct entertainment and communications companies. As they embark on this journey, operators are signing deals with content owners—who, in turn, expect and demand that their content be safeguarded while it is on the network. For operators that traditionally have focused largely on transmitting voice and data, content represents both a huge opportunity and a challenging new responsibility. To respond effectively to each, communications companies need to look beyond the technology and focus on the key processes that will keep content secure.

by Quentin Orr and Steve Woolley

Picture the scene. Two established but historically very different communications companies—a European-based cable company and a traditional fixed-line telephone operator located in Asia—are each seeking the best way to transform their business for the future. Let's call them Operator A and Operator B. Both companies know that their future profitability and even viability depend on migrating successfully into the multi-product, content-rich entertainment and media services marketplace.

Operator A, the European cable provider, decides that speed to market is of the essence in getting into this fast-moving, new environment. So it sets out to develop new, content-based products and services rapidly on the basis of its legacy infrastructure, using a range of specialist, external technology vendors, consultants, and third-party content providers for help in bringing its new offerings to market as quickly as possible. Long-term strategic planning for content management, security, and standardization takes a back seat in the rush to roll out basic new services and grab first-mover advantage.

In contrast, Operator B—the Asia-based telephone operator—decides to leapfrog the competition by focusing on product differentiation, and to enter its local market with an emerging and largely untested IPTV (Internet protocol television) offering. Its plan is to use still-evolving, leading-edge technology to support sophisticated, content-rich services, while also trying to establish a framework for managing such longer-term issues as standardization and skills.

A tale of two operators?

Of those two contrasting approaches to the same market pressures, which one wins? Unfortunately, the answer to date is neither of them. Operator A has succeeded in coming to market, but with a range of services that users and analysts feel lack innovation and coherence. The company also has become heavily reliant on external vendors, and only now is starting to appreciate the longer-term security, operational, and skills challenges it faces in the content-rich world.

In contrast, Operator B has a firmer grasp of the longer-term issues. But the size and complexity of its initial product set, and delays in the development of the new IPTV software, have slowed down the process of bringing the new services to market. As a result, Operator B has found its IPTV services stuck at the pilot stage and has been forced to postpone its launch plans as it seeks to fix a series of complex technology issues.

Clearly, these hypothetical stories represent two extremes in operators' approaches to the new, content-rich world of media. However, while their approaches appear different, both companies ultimately came up against a common stumbling block. Both found that it is vital to focus on getting the key processes right—and not to rely purely on technology, whether new or legacy, to protect and control the valuable content flowing across their networks.

Indeed, the choice of approach to the multiproduct world has major implications for operators' future ability to maintain the security of content. Security is absolutely critical in sustaining the new service model built on that content.

The challenge of content

The difficulties both fictional operators faced reflect the fundamental challenge most communications companies face today. Traditionally, they have been engineering-based businesses, focused on maximizing the availability of their networks. Their culture and mind-set have centered largely on using technology as a tool to solve most of the operational problems they encounter. Now, as they move into the content world, the limitations of a technology-focused perspective are becoming apparent.

Operators need to address this issue as soon as possible because they are spending significant amounts of capital to build out their network and content management systems. As they do so, they know that the choices they make now will stay with them for many years to come. They also know that it will become prohibitively expensive to make significant changes to this infrastructure in later years, when the pressure to achieve and maintain profitability will be at its highest.

So, as they formulate their strategies as content distributors, operators need to ask themselves some key questions, including:

- What should we focus on now as we build out our networks for the future?
- What are the content management issues today?
- Do we have the right people and processes in place to manage this ourselves after our early dependence on technology vendors ends?
- Have we adjusted our policies and procedures to guide decision making in a multiproduct environment?
- Is content security a key discussion point as we develop new systems and processes?

The answers will shape an operator's entire approach to acquiring, securing, and distributing content. And the first base for any content strategy must be the ability to keep content secure. Without that, there is a real risk that the opportunities presented by the multiproduct world not only may be missed, but also may be subsumed by liabilities and disputes with content suppliers.

Operator/content dynamics

To chart the right path forward, it is first necessary to take a step back and examine the emerging dynamics of the relationship between operators and content owners—both of whom face daunting challenges to their business goals.

On the content side, content owners perceive real threats to their existing revenue models both from piracy and from the impact of ongoing changes in consumer behavior. The content owners do recognize they need to adapt to consumers' changing preferences. They also know that adapting will mean investing in innovations, such as making more content available for time-shifted viewing and making content more portable. Such shifts can be summed up as enabling consumers to watch what they want, when they want, and with whatever device they want. The revenue opportunities presented by such a model are exciting but fraught with uncertainties.

On the other side, distributors—initially cable companies but, increasingly, operators as well—have invested heavily in infrastructure that is technologically capable of carrying rich content, and that provides the potential for considerable and growing cash flow. The bottom line is that they want to gain access to as much high-quality content as possible for distribution, and to pay content owners as little as they reasonably can. The problem for most communications companies is that their existing back-office infrastructure, even where it is now stable, is immature with respect to protecting content.

So, there are clear competitive tensions in the market. What is more, there is a risk of those tensions continuing to hinder the availability of digital content, due largely to divergent viewpoints on either side. On the content owners' side, many have neither encoded their entire catalog for digital distribution nor negotiated digital distribution rights for their content. Their initial reluctance and cautious approach to digital distribution more readily reflects the fact that, despite repeated attempts, they have not agreed with the distributors on a mutually satisfactory revenue-sharing model.

Movie studios, specifically, are also fully aware that the threat of piracy has undergone a step-change from “linear” mechanical copying of VHS tapes to “viral” sharing of digital files over the Internet. Yet studios are skeptical of the ability of distributors to protect their digital content from piracy by both consumers and, to a lesser degree, employees. Fanning the flames of content owners' fears about piracy is their own inability to protect their content even before they release it to movie theaters.

Operators face equally challenging issues on the distribution side. The technology for the digital distribution of content is immature, particularly in terms of the lack of end-to-end *de facto* industry standards for either digital rights management or encryption. As a result, operators cannot easily demonstrate the level of due care needed to allay the fears of the content owners. Content owners simply will not accept operators promising to protect the content, but not agreeing to be held to any standards or audits. And, as content deals and partnerships become more

extensive, the potential liabilities from failures in content security could be very heavy indeed for operators—possibly even crippling their businesses financially.

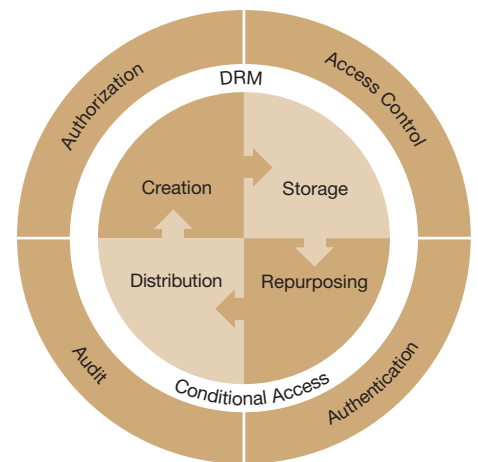
Looking beyond technology

In such circumstances, it is clear that rolling out services and technology like video on demand in a hurried manner, and without a lot of advanced thought on controls, monitoring, and reporting, is both shortsighted and highly risky. To position themselves for success in the multiproduct future, operators must look beyond the technology aspects and focus strongly on embedding the right processes and people—both of which are equally critical to the successful protection and security of third-party content. To gain focus, operators should step back from current operations and ask themselves the following questions, which might highlight the tell-tale signs of exposure:

- Do you have policies in place to address how people gain access to content?
- Do you have a framework in place to identify and manage the risks of content security?
- Do you have decentralized organizations that operate differently, by differing rules and management philosophies?
- Do you monitor the movement of content throughout your organization to quickly identify unusual patterns?
- Are you highly dependent on third-party technology vendors to support your systems? If so, do you have processes in place to monitor what they are doing on your systems?
- In the event of an incident, do you have processes in place to enable you to understand what happened and identify your vulnerabilities?
- Do you have technology architecture standards that dictate the methods and configurations for deploying new supporting technology in your environment?

As we have already pointed out, given their history as infrastructure players, this

Figure 1: Recommended content security framework



Operators must put a framework in place that supports digital rights management (DRM), and that enables them to understand the risks surrounding content and develop the capabilities and processes to mitigate those risks.

holistic perspective requires a change of mind-set and culture for traditionally engineering-based operators. They now must become adept at the entire content management and distribution life cycle, ensuring that they know at every stage exactly where the digital content is, who has access to it, and for what purpose.

A typical framework for content security is illustrated in Figure 1. As the graphic suggests, establishing this control requires operators to understand their risks and develop a number of capabilities and specific processes to mitigate those risks. Processes might include formal authorization processes before employees or business partners are given access to content; two-factor authentication methods to get access to high-value content; continual monitoring of content management systems; and pressuring technology vendors to build the best available security into their applications before they go live. With respect to individuals' capabilities, whether an operator has a linear video or a fixed telephone line heritage, many of its people may need training to understand the new challenges associated with a network-based content management and delivery system.

On a higher level, establishing control means operators must avoid becoming

overly reliant on the promises and hype surrounding the claimed benefits that technology can deliver for their business. It means accepting that technology merely facilitates effective content security—and that, for technology to fulfill this role, the operator first must have the processes, operations, and people in place to make use of the right technology tools. Such processes include proper authorization and auditing, supported by technology that can provide authentication and access control, to allow content to move through the organization in a controlled manner. And, establishing control means operators being ready and willing to submit themselves to the scrutiny of content partners who demand hard evidence that their assets are secure.

As operators strive to achieve content security, a further hurdle for many of them lies in the disparity and relative lack of connectivity among their existing systems. This situation, which mirrors that in many cable companies, tends to encourage bolting on various systems, including content management and security, as additional solutions. Again, this approach can hinder the ability to take a holistic perspective and it raises the risk of directing insufficient attention to and investment in the checks, balances, and governance processes needed for effective content security.

Models to follow

As communications companies implement their strategies into operations, what models or templates might they choose to follow? One useful starting point may be to examine how the major movie studios have tackled the issues of content security and piracy by building specific specialist capabilities.

Most of the leading studios have established expert teams that focus exclusively on content security and processes, and that most often operate independently of the traditional mainstream IT department. As operators and other digital distributors handle greater and greater volumes of high-value content, and do so increasingly in real time, we believe they should consider

developing dedicated capabilities of this kind internally. By concentrating solely on protecting content, rather than that being one responsibility among others, such teams avoid the distractions and lack of clear lines of accountability that can hamper an operator's performance in this area.

In assembling a team, operators should aim for a combination of technical and business skills. The head of a team would need to interface internally with product development and engineering teams as well as externally with content owners, technology vendors, and their attorneys. For the business skills, it might be helpful to look outside the organization to other industries more familiar with content negotiations and usage rights and obligations. For the technical capabilities, it may be possible to find the right individuals within the existing engineering or IT security functions, provided they do not carry any pride of ownership over the existing systems and processes. We suggest starting small with a team of two to three people and expanding as the volume, value, and various types of content increase.

A rigorous, focused approach will become all the more valuable over the coming years, as joint ventures, collaborative partnerships, and information sharing between operators and content providers continue to increase in number, scope, and complexity. Such arrangements often involve sharing or transmitting content among multiple partners, networks, entities, and teams—creating security risks and vulnerabilities at every hand-over point, as well as in the end-user distribution arena. In this kind of environment, the value of an effective process for monitoring and tracking content will truly come to the fore. And, as we have already pointed out, the contractual liabilities for a security failure could be onerous.

No silver bullet

For today's operators, the overall messages are clear. Content security is critical to operators' business models as future multiproduct providers. And while technology plays a key role in operators' content security, it is just one element among many. In other words, technology is not a silver bullet for content protection—and to think otherwise is not just misguided, but dangerous. The need to focus on processes is all the more critical for operators that possess, as many do, a disparate and largely unintegrated legacy IT architecture. In these circumstances, the only way to pull together all the strands, short of replacing complete systems, is through robust, overarching processes and controls.

However, operators must balance the need for processes with commercial time pressures. Upon deciding to enter the multiproduct content space, they need to move as quickly as possible. With this in mind, operators tackling content security must focus on doing so at high speed while also ensuring effective and comprehensive execution. Also, given the shifting and evolving threats to content security resulting from the rollout of broadband IP and increasing consumer empowerment, operators should constantly review and fine-tune their overall approach and specific processes to ensure that they remain fit for purpose.

Digital content opens up new vistas of opportunity for operators—but also brings risks and responsibilities that lie outside the traditional scope of their business and capabilities. Technology is part of the answer. But unless the right processes and governance are in place as well, an operator that embarks on the digital journey risks far more than it needs to.

Quentin Orr is a director and Steve Woolley is a partner in PricewaterhouseCoopers' Communications Industry group. For more information, contact Mr. Orr by phone at [1] 267 330 2699 or by e-mail at e.quentin.orr@us.pwc.com; or Mr. Woolley by phone at [61] (3) 8603 3808 or by e-mail at stephen.woolley@au.pwc.com.