Cybersecurity: keeping content, brands and people safe online is everyone's business—and a strategic imperative

Cybersecurity: the 15-second download

5 The most valuable assets any entertainment and media company possesses—its 'crown jewels'—are its content. If they're stolen, compromised or used inappropriately, a business risks significant lost revenue and deep damage to its reputation and future revenue potential.

10 Despite the crucial importance of cybersecurity, it doesn't always receive the board-level attention it deserves, partly because it's often seen as a technology rather than business issue. Boards need to work in a coordinated way to recognise their exposure and potential impacts from cyberattacks.

15 Companies can enhance their ability to prevent and detect cyber breaches through three steps: making cybersecurity everyone's business; strengthening the ecosystem; and identifying and protecting their most critical assets. A collaborative approach underpinned by appropriate technology tools can be the best solution.

Protecting the company's key assets …

An entertainment and media company's most valuable assets—its 'crown jewels'—are its content. These are the assets that drive cash flows, competitive advantage and shareholder value. If they're stolen, compromised, or used inappropriately, a company risks significant lost revenue and deep damage to its reputation and future revenue potential.

So entertainment companies are seeking better ways to protect content, both pre- and post-release. Pre-release protection focuses on shielding video and other content so it isn't stolen or leaked before the official release, damaging viewership and revenues. Content protection is equally important post-release stage to guard against losses from piracy.

Media companies face the same need to protect content, but for different reasons—since alongside the risk of lost revenues from content theft they also face issues around journalistic integrity. So protecting intellectual property (IP) from unauthorised access may be not just a business imperative, but possibly a matter of life and death for sources.

At the same time, the information assets that entertainment and companies need to protect are expanding, raising new business issues and imperatives. As companies gather more and more data on their consumers, effective cybersecurity to safeguard this highly sensitive information and maintain its privacy is increasingly vital for retaining the trust in their brands. As a result, consumer data is set to become part of each company's 'crown jewels'—if it has not done so already.

… should not be a 'sleeper' issue

So the stakes are high and rising. But despite this, the security of digital information—cybersecurity—doesn't always receive the attention it deserves at board level. All too often, at least until a major breach occurs, it's still viewed as the responsibility of the technology team. But the reality is that effective information and cybersecurity are the linchpin for safeguarding an entertainment and media company's most valuable assets.

Like businesses in other industries, they're also finding it hard to stay a step ahead of the attackers, as cyberattacks continue to grow in number and sophistication. Indeed, it's no longer a question of *if* a business will suffer an incident, but *when*. In *The Global State of Information Security® Survey*[1] of more than 9,600 global executives,

1. www.pwc.com/gsiss2014

pwc

Fig. 1: Entertainment and media businesses detect more security instances

Average number of security instances in the last 12 months

Source: *The Global State of Information Security® Survey 2014*
The Global State of Information Security® is a registered trademark of International Data Group, Inc.

entertainment and media respondents reported a 50% jump in incidents detected over the past year (see Fig. 1). They also reported that compromises of employee information had almost doubled, putting valuable relationships at risk.

Furthermore, the threats are increasing at a time when businesses' vulnerabilities to attack are also on the rise, due to trends such as greater digital connectivity between companies in 'business ecosystems', an increasing dependence on technology and connectivity, and the fact that safeguarding *all* data at the highest level of security is no longer realistic.

Strategies for strengthening the business

Faced with this situation, the leaders of entertainment and media businesses are sometimes unsure where to focus their efforts. The key is that all board members should work in a coordinated way to recognise the exposure and potential impacts from the evolving, targeted threats to their business model, taking into account the deep motivations and capabilities of their adversaries. Working on this basis, the company might take some or all of the following three actions.

First, **make cybersecurity everyone's business**. It's crucial to elevate the role of information security in the organisation and emphasise that it is a strategic business issue, not just a technology function. Cybersecurity should be as much a concern to C-suite executives as it is to the IT team. It is also the business of employees, contractors, third-party vendors, and other ecosystem partners—all of whom should at least have a basic understanding of how the company protects, detects and responds to cyberattacks on people and information.

Second, **strengthen the ecosystem**. The integrity and stability of any entertainment and media business is now more dependent than ever before on the other companies in its ecosystem. Because of the interconnected nature of the ecosystem and the growing reliance on collaborators, vendors and third parties, organisations must integrate these external partners into their cybersecurity strategy. This means everyone needs to understand not only what the policies and processes are, but also why they need to adhere to them.

Although third parties in the ecosystem are always a concern, some companies have been surprised to discover that the biggest problems are often caused by their own employees. For example, companies may find that workers lack even a basic awareness of the information security risks to which they're subjecting the business when they don't follow policies—for instance, they fail to change default passwords, leave their computers on when they go home, or open spam emails using company equipment.

Third, **identify and protect the most critical assets**. As we highlighted earlier, not all information assets are equal in value. So companies must determine which information assets are their 'crown jewels' and provide those with enhanced protection. This

entails knowing not only which assets they are, but where they're located at any given time, and who has access to them. If these assets are being transferred to third parties, there should be assurances that they're being securely handled.

Towards a new model

As companies take these steps, many face the challenge that the approaches they use to manage cybersecurity risks have not kept pace with the escalating threats. This is partly because the traditional information security model—essentially compliance-based, perimeter-oriented, and reactive—does not address the realities of today's environment. As a result, companies have spent billions of dollars on security products and services that are built on outdated security models.

While entertainment and media companies have focused primarily on preventing theft of pre-release content and monitoring for post-release piracy, the limitations of this approach are becoming increasingly apparent. Alongside a focus on prevention, they also need to be able to detect and respond to security incidents. Furthermore, while widespread digital transformation has opened up new vistas of opportunity for companies, it has also done the same for cyberattackers. So businesses should in turn exploit the potential of digital to improve their ability to protect content and detect attacks.

Taking the example of a movie studio's 'digital dailies' of a forthcoming blockbuster release, the studio could now distribute these vital assets to authorised parties—producers, directors, special effects partners and so on—complete with a new lightweight digital 'fingerprint', and a list of pre-approved locations where the content is permitted to go. This would enable access to the content to be blocked if it were sent to an unauthorised cyber location. And monitoring the fingerprint at the carrier level would help to track where the pre-release content went, enabling immediate identification of breaches or near-breaches.

At root, the barriers to effective cybersecurity are more around people and behaviour than technologies and processes. A collaborative approach, under which the various participants in the digital value chain share information and pool resources—while maintaining protection and vigilance through appropriate technology tools—can be the most cost-effective solution, while also delivering tangible security benefits for everyone involved.

Ten questions to ask:

1. *What are the most important digital assets in your business?*
2. *How do you protect them against cyber intruders?*
3. *Do you know at any time where those assets are and who has access to them?*
4. *Do you know who might seek to benefit through unauthorised access to your assets—especially content?*
5. *Does your business have a risk-aware culture embedded throughout the workforce?*
6. *How often do your board members discuss cybersecurity issues?*
7. *How do you assess and verify the security of your partners in your business ecosystem?*
8. *Are you confident that your internal staff and external partners' staff adhere to your security processes—and understand why they need to do so?*
9. *When did your business last experience a cybersecurity incident?*
10. *How did you respond—and what plans do you have in place to respond to cyber breaches in the future?*

Outlook insights: an analysis of the Global entertainment and media outlook 2014–2018
www.pwc.com/outlook