Your World First

C/M/S/

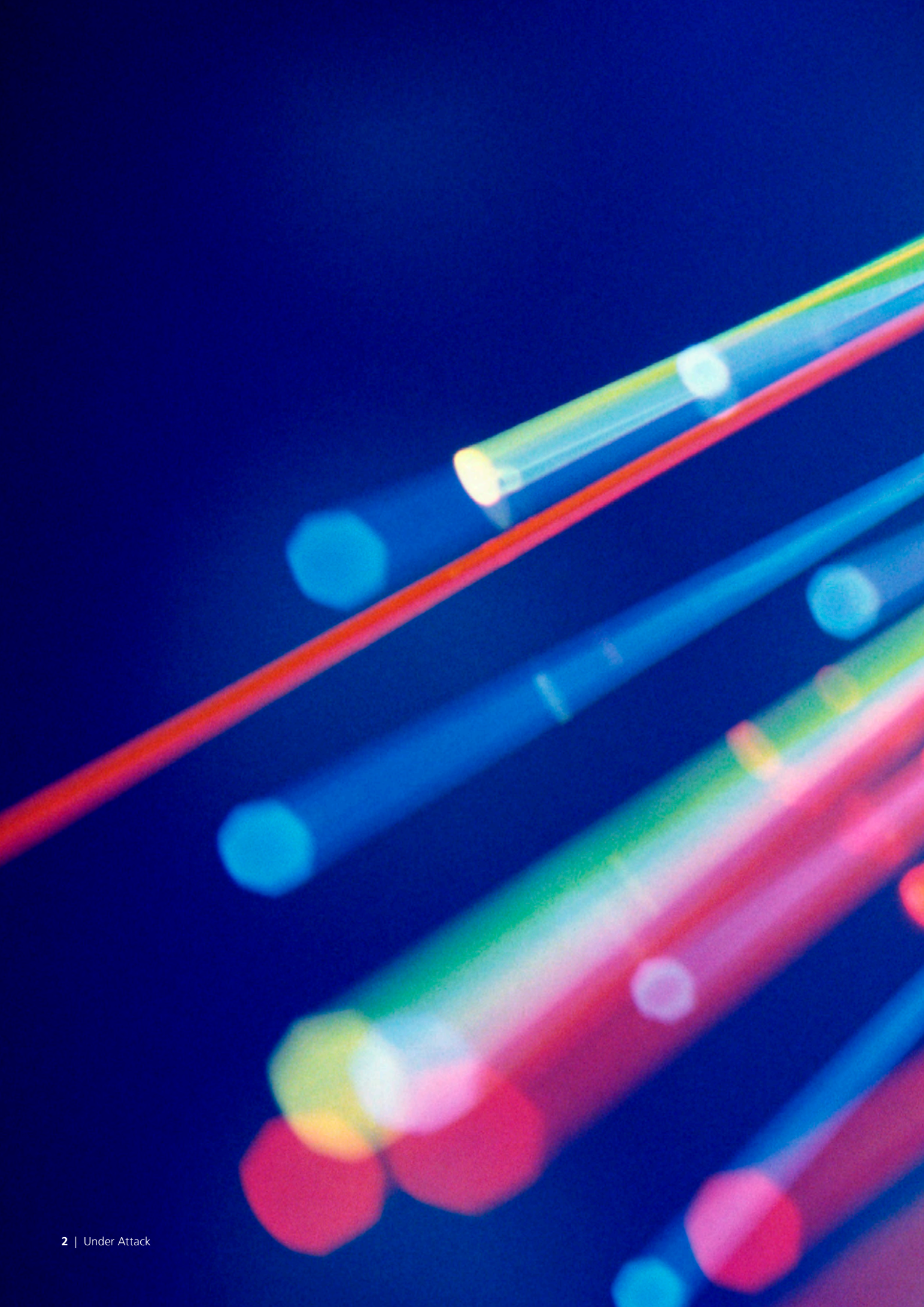
Law.Tax

Under Attack

A practical cybersecurity toolkit for media companies

November 2017

Published at the CASBAA Convention in Macau



Contents

5 Introduction: Media "Under Attack"?

7 The Cybersecurity Threats Facing Media Companies

10 Your Cybersecurity Toolkit

20 Your Checklist

21 How CMS helps

Introduction: Media "Under Attack"?

On 8 April 2015, all twelve channels operated by French network TV5Monde went off air. In the coming hours, more systems were corrupted and destroyed. According to Director General, Yves Bigot, the situation worsened to the point where the network itself came close to "total destruction". "We were a couple of hours from having the whole station gone for good." The cause? A highly sophisticated cyber-attack.

TV5Monde was not the first media company – nor would it be the last – to fall victim to a cyber-attack. Prior to the TV5Monde hack, in November 2014, news spread online that the systems of Sony Pictures had been compromised by a group calling itself the "Guardians of Peace". A library of confidential documents, personal data of employees and valuable intellectual property, including unreleased movies, began to appear online. By mid-December, Sony had pulled "The Interview" from its initial release in US theatres in response to threats from the attackers. The attacks didn't stop there. HBO endured a torrid month in August 2017, during which it suffered a massive server breach, leaks of full episodes of unreleased shows (including episodes of Game of Thrones) and even the hijacking of its main Twitter account.

Unfortunately, these are not isolated incidents. Media companies are facing the threat of attacks from a range of sources, including hacktivists, cyber-criminals, nation states and even disgruntled employees. The total financial costs related to security incidents in 2016-2017 soared 81% year-on-year[1].

So what is behind this spike in attacks? Undoubtedly, the nature of the industry and the content it produces, whether it is news, entertainment, documentary or film, is such that some media companies will always be a target for malicious attacks. But there is more to it than that. The reasons to attack are increasing. As the industry goes digital, its digital assets, such as movie scripts, unreleased TV shows or employee data, carry an increasing value that appeals to international cyber-attackers. In addition, media companies are increasingly using third -party infrastructure and services to store and process data and content – and without the right safeguards in place, this can expose them to new risks. And with the shift to distributing content online via a growing range of connected devices, the attack surface is growing all the time.

> We were a couple of hours from having the whole station gone for good.
>
> *Yves Bigot, Director General, TV5Monde, on their 2015 cybersecurity incident.*

1 www.pwc.com/gx/en/issues/cyber-security/information-security-survey/entertainment-media-communications-industry.html

Within organisations, cybersecurity has shifted from a legal and compliance team responsibility to a board-level priority. The days when cybersecurity was a hypothetical risk have passed. Investments are being made in cybersecurity, up around 7% year-on-year within the entertainment and media industry, with the goal of closing the gap between cyber-defences and cyber-attackers. But despite these efforts, the attacks continue.

As a leading international law firm in the media sector, working with companies around the world, CMS has witnessed first-hand the cybersecurity threats facing the industry and the damaging impact that cybersecurity incidents can have on organisations. We have worked with companies across sectors on all aspects of cybersecurity, from developing an organisational strategy for cybersecurity through to pre-incident planning and post-incident response. We have seen how some organisations, with board-level leadership, have taken major strides forward to enhance protection, including best-in-class technical and operational measures – and we have seen how others still have a long way to go.

Through this work and our discussions with organisations and regulators around the world, we have developed substantial experience of best practice approaches across jurisdictions. Our intention in publishing this paper is to make a further contribution to the conversation about cybersecurity within the media industry and to share the benefit of our experience with media organisations.

We hope that you find this paper useful and look forward to continuing to work closely with our media clients around the world to ensure that the industry can continue to innovate and grow in a way that manages the cybersecurity threat.

Matt Pollins
Head of TMT and Commercial
CMS Singapore

> The days when cybersecurity was a hypothetical risk has passed.

The Cybersecurity Threats Facing Media Companies

Why is the media industry a priority target?

The media industry is a priority target for cyber-attacks. No fewer than 7,674 security incidents impacted entertainment and media companies in 2016-2017, a 26% increase year-on-year[2]. Of course, the media industry is not alone in facing attacks. However, there are several reasons why the media industry is a priority target.

The nature of the business

The nature of the media industry is such that it will always be a target for malicious attacks. Media companies produce and distribute content – and content can potentially be divisive or offend particular interest groups. This can lead to proactive or reactive attacks from interested parties. For example, the Sony Pictures attack was linked to North Korea, allegedly in retaliation against the representation in "The Interview" of a plot to assassinate North Korean leader, Kim Jong-un. The "Guardians of Peace" group, which claimed responsibility for the attack, threatened further attacks against both Sony Pictures and any theatres that showed the movie. Within a month after the attack, Sony Pictures took the decision to cancel the theatrical release – although it later allowed a theatrical and online release later in the year.

The broad distribution network

Media companies usually have broad distribution networks, often global, and they tend to have a very large customer base relative to other industries. This makes them a focus target for cyber-attacks. The news industry is a good example. If hackers can gain access to news websites or the social media accounts of news channels or their journalists, they have a powerful tool with which to spread false information (so-called "fake news") or to post divisive messages. This is a particular risk during periods of heightened political interest, such as election periods. The threat is not limited to "fake news" – it extends to the distribution of other malicious content via media networks, such as malware and ransomware.

Case Study 1: Sony Pictures, 2014

Date: The initial signs that systems had been compromised appeared in November 2014, although a purported member of the "Guardians of Peace" claimed to have had access to Sony Pictures' systems for more than a year.

Attack type: Malware

Impact: IT systems rendered inoperable, compromise of employee information and valuable intellectual property rights, including unreleased content. Within a month after the attack, Sony Pictures took the decision to cancel the theatrical release – although it subsequently allowed a theatrical and online release later in the year.

1 www.pwc.com/gx/en/issues/cyber-security/information-security-survey/entertainment-media-communications-industry.html

The valuable digital assets

Media companies hold highly valuable assets in digital form. The value of these assets makes them a key target for malicious attacks. The key targets for attacks include:

1. Valuable intellectual property rights. The content produced and distributed by media companies remains in high demand. Netflix reportedly has a USD 6 billion content production budget in 2017[3]; HBO is set to spend about USD 15 million per episode for the final season of "Game of Thrones"[4]; and the English Premier League's latest overseas broadcast rights deal totalled approximately GBP 3.2 billion. The phrase "content is king" is perhaps overused in media industry circles – but undoubtedly the value of content has not escaped the attention of cyber-criminals, who are more incentivized than ever to steal and monetise the crown jewels of the media industry.
2. Customer information. Media companies are interacting with consumers more than ever before – whether it is engagement via online platforms and social media, subscription and billing arrangements or understanding viewer behaviour to deliver targeted advertising or content. These interactions are generating more data than ever before. The shift to digital, and the data it provides access to, represent a huge opportunity for the media industry – but the valuable data also represents a potential treasure trove for cyber-criminals.

Third party infrastructure and services

Media companies are increasingly leveraging third-party infrastructure and services to support their operations. There are several reasons for this – from cost reduction via outsourcing through to accessing specialist products and services that media companies cannot develop in-house. Examples include:

1. A rapid shift to cloud services for the storage and streaming of media assets.
2. Digital delivery of content.
3. Use of outsourced technology services, such as uplink and playout.
4. Sharing assets with partners – such as OTT content aggregators, who typically require copies of programming well in advance of that programming being premiered.

Where managed appropriately, use of third-party infrastructure and services need not materially increase the cybersecurity exposure (and in some cases third parties actually provide services that enhance levels of security – for example, cloud services have the potential to be more secure than on-premises equivalents due to their billions of dollars in security investments). However, without the right safeguards in place, from security due diligence through to contractual protections, media companies are exposed because their security is only as strong as the weakest link in the chain.

Investment versus other regulated industries

For many years, industries such as financial services have been investing heavily in cybersecurity. Indeed, cybersecurity in financial services is driving the growth of the multi-billion dollar "fintech" industry. Media companies are certainly not standing still and attacks can affect even the most sophisticated organisations - but at an industry level, investment still lags a long way behind that in many other sectors. According to PwC research, in 2016-2017 there was a 26% increase in detected cybersecurity incidents but only a 7% increase in information security spending by media companies. Some media companies are under-investing in cybersecurity versus companies in other industries and that makes them a "low-hanging fruit" for attacks.

3 www.cnbc.com/2016/10/17/netflixs-6-billion-content-budget-in-2017-makes-it-one-of-the-top-spenders.html
4 http://fortune.com/2017/09/27/game-of-thrones-final-season-episodes-cost/

What are the common threats?

Cyber-attacks against media companies are evolving all the time but common patterns and strategies have emerged.

Common attack types

— Malware distribution
— Ransomware
— DDOS
— Compromising privileged accounts
— Using media networks to spread false or malicious information, e.g. "fake news"

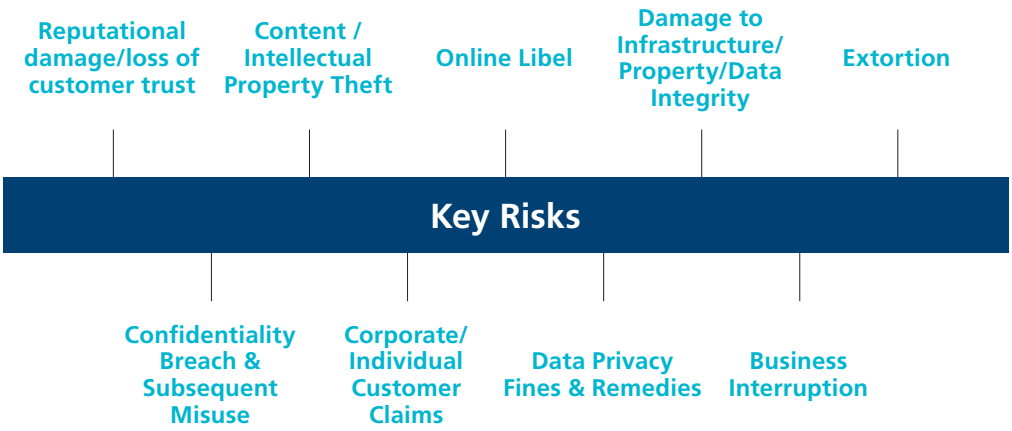
Potential assailants

— Cyber criminals
— Terrorist groups
— Kudos hackers
— Hacktivists
— Disgruntled employees or contractors
— Nation states

Fig. 1: Common attack types and potential assailants

What are the risks?

Risks associated with cyber-attacks range from the obvious – loss and corruption of data and intellectual property theft – to the less obvious but potentially even more damaging – regulatory fines and reputational damage.



Case Study 2: TV5Monde, 2015

Date(s): 8 April 2015, although the perpetrators first penetrated the network as early as January.

Attack type: Malware. According to the BBC, the perpetrators "carried out reconnaissance of TV5Monde to understand the way in which it broadcast its signals. They then fabricated bespoke malicious software to corrupt and destroy the internet-connected hardware that controlled the TV station's operations - such as the encoder systems used to transmit programmes."

Impact: All twelve channels operated went off air and its website and social media were compromised. According to Director General, Yves Bigot, the situation worsened to the point where the network itself came close to "total destruction". "We were a couple of hours from having the whole station gone for good."

Your Cybersecurity Toolkit

Overview

Based on our international experience, we have developed a four-pillar approach to managing cybersecurity risk for media companies.

Each of the four pillars is inter-dependent. For example, an understanding of legal obligations in Pillar 1 will inform your organisation's overall cybersecurity strategy in Pillar 2, which, in turn, will inform how you must work with third parties in Pillar 3 and respond when a breach occurs, in Pillar 4.

In the following sections, we look at each of the four pillars in more detail and provide a practical toolkit for managing cybersecurity risks. We then provide a checklist against which you can measure your organisation's progress.

Pillar 1: Understand your legal and regulatory obligations

As the threats increase, legal systems around the world are catching up, and this is imposing new compliance obligations on media organisations. Any cybersecurity strategy needs to be rooted in an understanding of your company's legal obligations.

Which laws and regulations apply?

The legal obligations applying to media companies fall into four broad categories:

1. Contractual and intellectual property obligations. Your organisation will probably be subject to contractual and intellectual property obligations. For example, if you are an international TV channels business and license content from US studios, you may be subject to stringent security requirements designed to mitigate the risk of intellectual property theft.
2. Privacy laws. These apply to cybersecurity incidents that impact "personal data". In most cases, this means data relating to individuals – such as name, contact details, billing information and employee data. Organisations have responsibilities under privacy and data protection laws to keep personal data secure, and to take certain actions if an incident occurs, such as notifying the regulatory authorities and/or affected individuals within a specified time period. Privacy laws do not apply to "non-personal" data, such as technical or operational data or the content of a movie script, and privacy is only one aspect of an organisation's overall cybersecurity exposure. Most countries have privacy laws, whether those are constitutional rights to privacy or comprehensive data protection laws, like Singapore's Personal Data Protection Act or the General Data Protection Regulation (GDPR) in the EU.
3. Cybersecurity laws. In response to the growing range of cybersecurity threats, policy-makers are introducing cybersecurity laws and regulations. They usually apply to operators of "Critical Information Infrastructure", which in some case may include broadcast infrastructure. The obligations include incident reporting, permitting regulators access to systems, and sharing information about cyber-threats. Depending on the nature of your operations and the jurisdictions in which you operate, some aspects of your infrastructure could fall within the definition of "Critical Information Infrastructure".
4. Media regulations. The media industry itself is regulated by sector-specific regulations and licensing conditions. These regulations may impose obligations that are relevant when it comes to cybersecurity – for example, pay TV platforms will often have specific obligations to their subscribers.

In focus: GDPR

What is GDPR? The EU's General Data Protection Regulation. It is a stringent new privacy law that will take effect from May 2018.

Our organisation is not in Europe – do we need to know about it? Most likely yes. GDPR is extra-territorial. It applies when organisations offer goods or services to individuals within the EU or monitor the behaviour of people within the EU. If your organisation does these things, it is subject to GDPR and must be compliant by May 2018.

What does it require? Organisations must comply with several new obligations when it comes to managing personal data, such as carrying out privacy impact assessments and reporting data breaches to authorities. It is much more stringent than previous privacy laws.

What are the sanctions? GDPR has teeth. The maximum fine, for serious breaches, is 4% of worldwide turnover or 20 million Euros. For a global media company, fines for serious breaches could potentially run into the billions of dollars.

What do these require us to do?

The requirements will differ depending on the nature of your operations and the locations in which you do business. However, we have extracted some principles which, in our experience, apply broadly across most jurisdictions.

1. Have policies and processes in place

Organisations need to have policies and processes in place to ensure compliance. These would typically include:

— a data security policy based on regulatory and contractual obligations;

— appropriate privacy policies and consent mechanisms, to ensure that the individuals whose personal data is collected understand and consent to the use of their data;

— carrying out a "privacy impact assessment" to weigh up the privacy impacts of a particular service or campaign and the measures needed to mitigate any associated risks; and

— training for staff to ensure that policies are applied in practice.

We expand on these requirements in Pillar 2.

2. Keep data secure

Your organisation will likely be subject to obligations to keep data secure, whether under privacy laws, cybersecurity laws, broadcast licence conditions or contractual commitments to third parties. The obligations will depend on the nature of your business and the jurisdictions in which you operate but there are some common trends:

Type	Description	Examples
Physical security	Many security incidents relate to the theft or loss of physical equipment, such as computers being stolen or hard copy records not being disposed of. Your organisation should have processes in place to protect physical assets as well as digital assets.	Alarms and security systems, CCTV, records disposal.
IT security	This is a constantly evolving area so the measures that are best practice today may not be best practice tomorrow. However, there are some baseline measures such as data encryption that are now an expected minimum. In addition, there is a growing range of national and international security standards developed by independent third parties, such as those issued by the International Standards Organisation (ISO), which can be used to measure your organisation's IT security against good industry practices.	Encryption, certification against ISO standards.
Personnel	You should have measures in place to ensure that only authorised people can access personal data and to ensure that those people only act within the scope of their authority.	Staff background checks and security vetting for those accessing privileged accounts, IT usage policies and training (e.g. as to the risk of phishing attacks).
Organisational	You need to build a culture of security within your organisation. This includes having an organisational security strategy. We expand on this in Pillar 2, below.	Development of an organisation-wide security strategy. See Pillar 2, below.

Fig. 3: Examples of "baseline" security measures for media companies.

3. Manage third parties

Data laws, as well as contractual commitments, typically require organisations to take responsibility for the people they share data with. For example, if your organisation works with a technology vendor and shares data with that vendor, your organisation has responsibilities to manage that vendor and ensure they keep data secure. The vendors themselves need to play their part by demonstrating how their security measures meet the necessary standards. We expand on how you can manage third parties in Pillar 3, below.

4. Notify if a breach occurs

Data laws increasingly require organisations to notify if a breach occurs. For example, the EU's General Data Protection Regulation (GDPR) will require organisations to report certain types of data breach to regulators, and in some cases to affected individuals, within 72 hours of becoming aware of the breach. At a contractual level, you may also be required to notify affected partners.

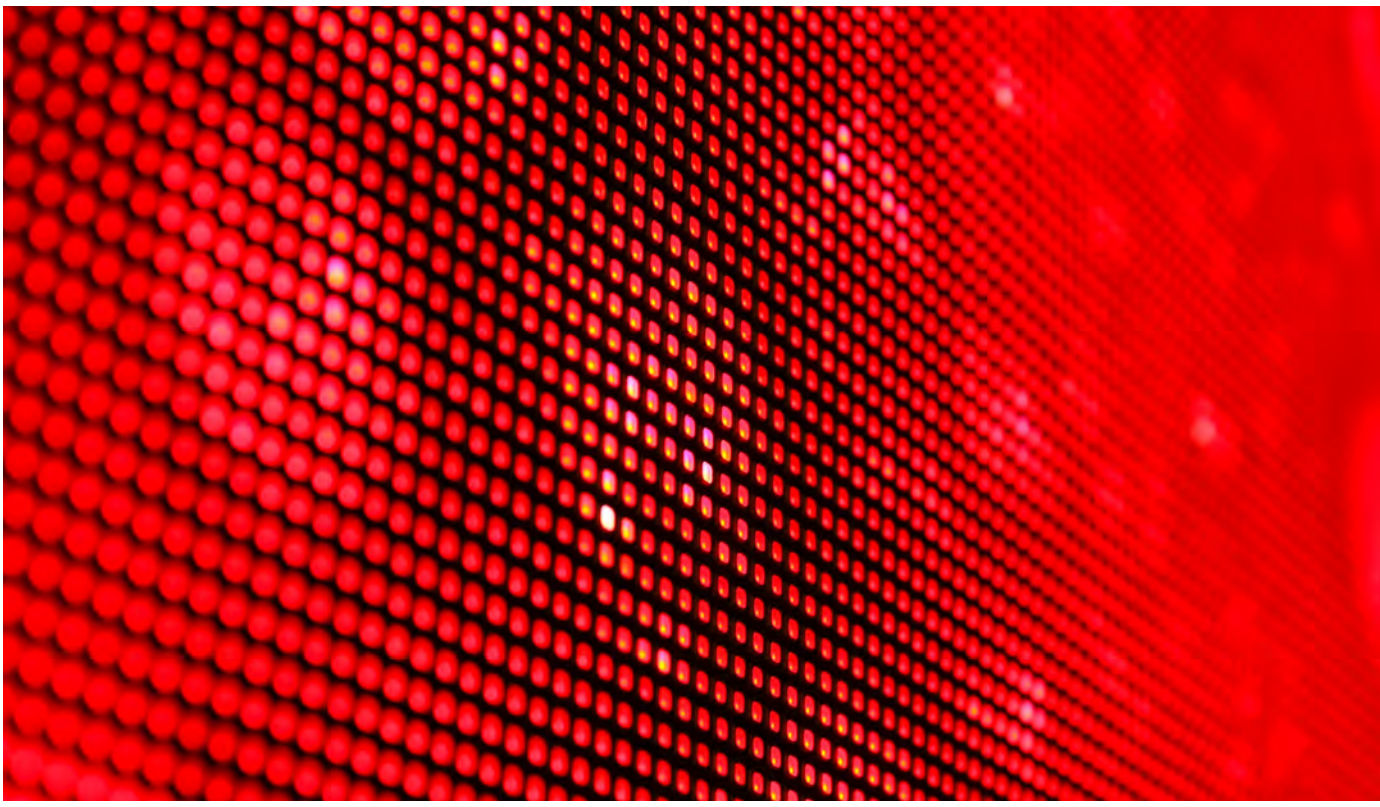
What are the penalties?

Although the financial penalties are potentially large and must be taken seriously (e.g. GDPR carries a maximum fine of 4% of worldwide turnover, or 20 million Euros), the greater concern for media companies will often be:

— loss of **valuable intellectual property rights** – in the media industry, leaks of unreleased movies, scripts or TV shows could lead to substantial lost revenues;

— **contractual exposure** – a cybersecurity incident could place your organisation in breach of contractual obligations to third parties - for example, a licence deal with a US studio may require your organisation to implement security measures to prevent hacks occurring and this could lead to a contractual damages claim and the termination of your deal; and

— **reputational fallout** – breaches often make the news but even when they don't, a common sanction applied by regulators is to "name and shame" organisations that fall foul of the regulations. The reputational impact of a cybersecurity incident can be difficult to quantify and can range from loss of subscribers to longer-term brand damage.



Pillar 2: Build your strategy

1. Form a multi-disciplinary Cybersecurity Team

A multi-disciplinary team needs to be put in place and given responsibility for managing cybersecurity within the organisation. No single business unit can manage the project alone – representatives from across business units, as well as external advisors, will need to be involved.

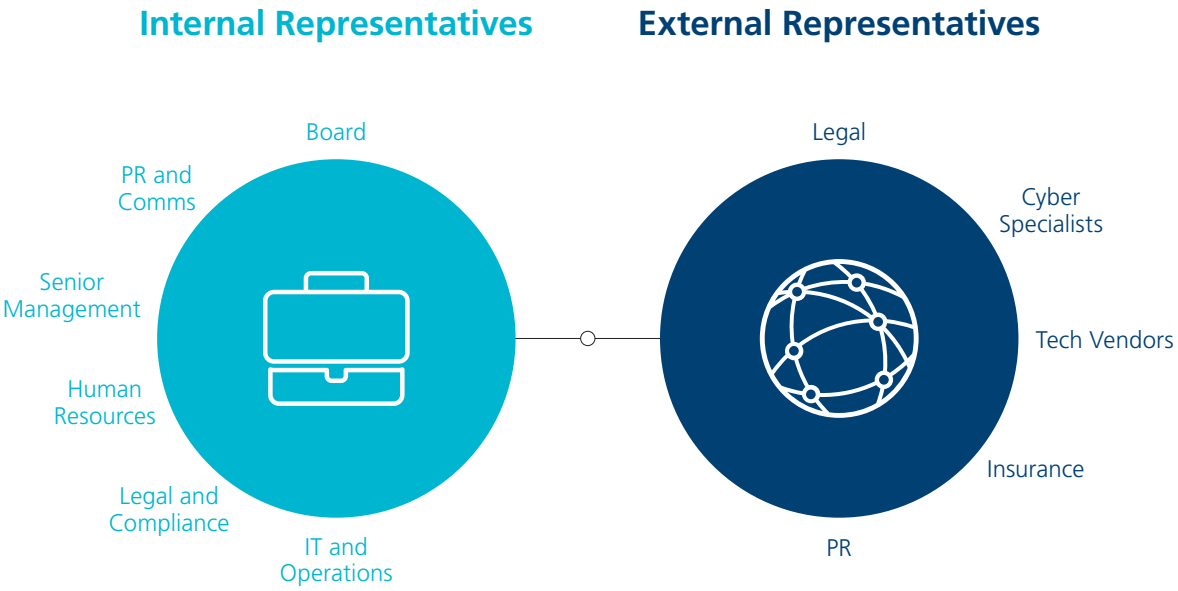


Fig. 4: A multi-disciplinary cybersecurity team

2. Build a benchmark and audit against it

Having built the team, it is essential to have a snapshot of where your organisation stands today and the steps it needs to take to enhance its cybersecurity. Your legal advisors should be able to assist with this. Our recommendations are to:

— **build a "benchmark" standard** against which you will measure your organisation's cybersecurity practices – this would typically be based on:

- legal and regulatory requirements in the jurisdictions in which you operate;
- international best practices such as ISO security standards; and
- specific security measures imposed on your organisation by contract – for example, by US studios under content licence deals;

— carry out an **audit** of your current cybersecurity practices; and

— perform a **gap analysis** of the outputs of the audit against the benchmark, to determine where the organisation is falling short of the required standards.

3. Develop and implement a rectification plan

Having built the benchmark and audited against it, you are now in a position to develop a rectification plan to address any weaknesses. The content of the plan will depend on the outputs of the audit but, in our experience, would typically include:

— the need to implement **enhanced technical measures** to address identified weaknesses, such as encryption of data;

— the need to develop **data security policies**;

— the need to develop a **cybersecurity incident response plan**;

— the need to build an agreed **PR and communications plan**, to apply when a cybersecurity incident occurs;

— the need for **personnel training**; and

— the need to implement **enhanced physical security measures**.

Needless to say, priority areas (such as material security weaknesses exposed during the audit process) must be addressed first. The plan needs to have clear responsibilities tagged to specific individuals and teams, together with firm deadlines.

4. Consider cybersecurity insurance

Many organisations are now considering cybersecurity insurance, and several large insurers are starting to offer coverage. This is a new field within the insurance industry and one that should be considered as part of your organisation's overall insurance strategy.

5. Communicate and train the team

A strategy is only effective if it is actually applied in practice. Developing a plan is only the first step. Organisations need to develop a culture of security across the business, with top-down support. This needs to be supported by frequent training for all relevant personnel across the business. Not only does frequent training reduce the risk of issues occurring, it also potentially reduces the exposure of the organisation if a breach does occur, as regulators will often look at training as part of their assessment of whether the organisation had appropriate measures in place. For large organisations, in-person training can be a logistical burden, so companies such as CMS are increasingly offering eLearning solutions that can be immediately rolled out across the organisation.

6. Test it

Just as regular drills are a necessary measure in preparing for a fire, so should organisations test their cybersecurity plans regularly to ensure that they are fit for purpose and that each relevant team member knows what is required of them. As a starting point, we recommend carrying out a cybersecurity incident workshop, based on a rolling breach scenario, with representatives from senior leadership, legal and compliance, HR, PR and communications and IT and operations.

7. Keep it under review

Cybersecurity is a rapidly evolving area and organisations cannot afford to stand still. The cybersecurity strategy needs to be kept under constant review to ensure it addresses the latest threats, as well as the latest legal and regulatory changes impacting the organisation.

Pillar 3: Manage your partners

Why are your partners relevant?

Media companies are increasingly leveraging third-party infrastructure and services to support their operations, from cloud services and digital delivery to outsourced uplink and playout. And the nature of the media industry is such that media assets will often have to be shared with partners – for example, a rights owner will need to share media assets with the platforms that distribute its content.

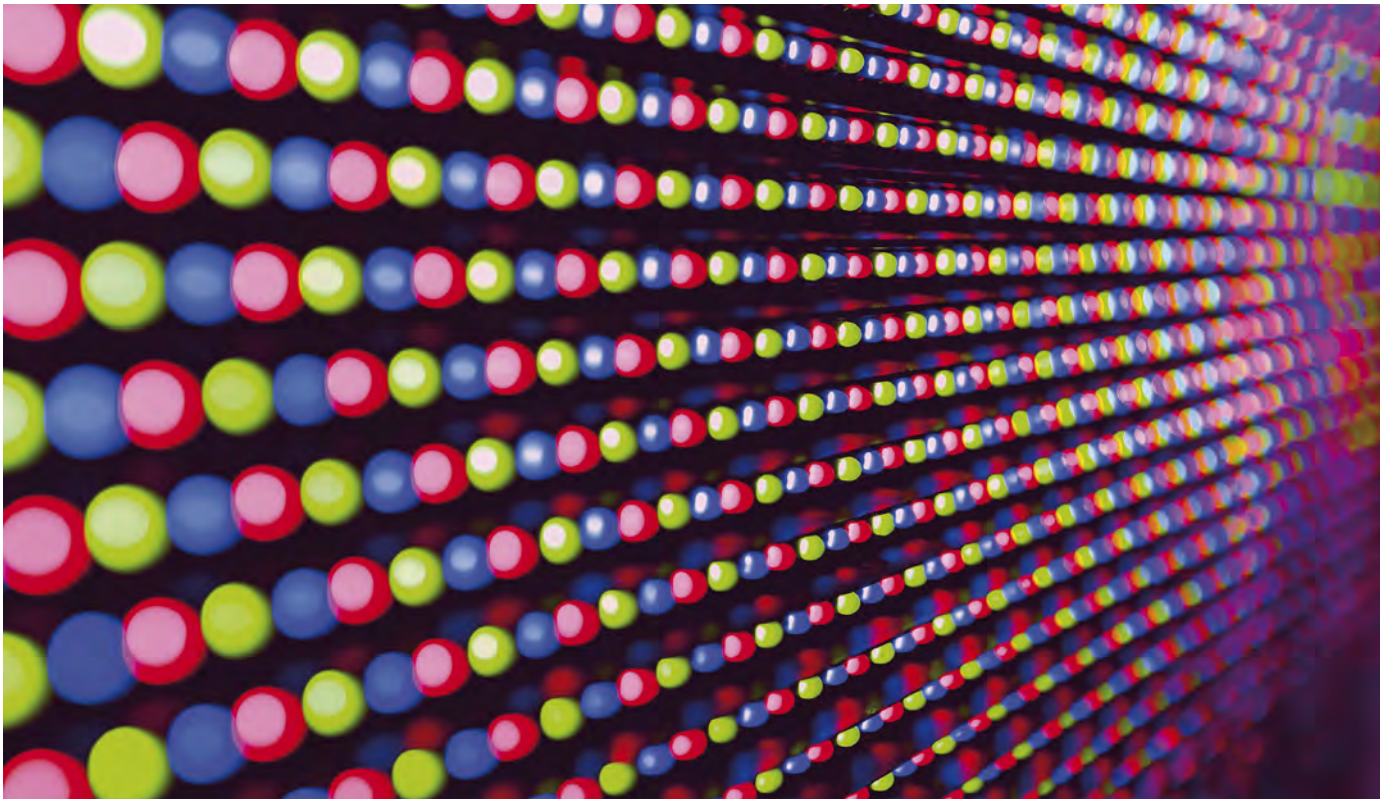
Any cybersecurity strategy is only as strong as the weakest link in the chain. If the partners with whom you share data or content do not have strong security measures in place, then your organisation is exposed.

So what can your organisation do to manage the risks of working with third parties?

Do appropriate due diligence

You should do appropriate due diligence on your partner. This would typically include an assessment of the following:

1. **Security standards.** Ask for information about their security standards and policies and assess these against your organisation's own standards and policies. Are there any weaknesses?
2. **Track record.** What is your partner's track record in security? Have they previously been the subject of a cybersecurity incident and, if so, what measures have they put in place to minimise the risks of incidents occurring in the future?
3. **Monitoring and control.** What measures will be in place to ensure that you retain control? For example, if it is a cloud solution, do they provide a dashboard that notifies you of service performance and security incidents? If not, you may lose visibility and an incident could occur without you being aware of it.
4. **Location transparency.** Is your partner transparent about where your data and content will be stored? Some laws require you not to transfer data (particularly personal data) outside of a particular country or region unless certain measures are in place. If you don't know where the data is, you might be in breach without knowing it.
5. **Business continuity.** Does your partner have a business continuity plan? To the extent that your operations are intrinsically linked with those of your partner, does their plan dovetail with your own plan? Have you considered joint testing?
6. **Conditions on who they share data with.** Does your partner work with sub-contractors or sub-licensees? Again, your cybersecurity is only as strong as the weakest link in the chain. You will want to impose conditions on who they can share data or content with, so that you have visibility and control.
7. **Conditions on termination.** You should be prepared for a scenario where the relationship comes to an end. What happens to your information – is it returned to you and then deleted, or does your partner retain a copy? If they retain a copy indefinitely, the associated risks of a security incident also continue indefinitely.



Get a robust contract in place

Having done your due diligence, you need to have a robust contract in place. Of course, security is only one aspect of a contract, alongside the key commercial and legal terms – but it should certainly be an important term where you are sharing data or content. The appropriate terms will depend on the nature of your relationship with the partner – for example, the terms for a cloud hosting deal will be very different to those in a content licence agreement. You should take advice from your legal counsel on this but the relevant terms are likely to include the following:

1. **Intellectual property** – clear parameters as to how content can be used
2. **Privacy** – commitments to comply with privacy laws
3. **Security** – minimum security controls – such as compliance with your IT Security Policy
4. **Breach notification** – an obligation to notify you if a data breach impacting your organisation occurs
5. **Availability** – uptime commitments
6. **Business continuity** – obligations to notify you of business continuity incidents impacting your organisation and to deploy a business continuity plan
7. **Confidentiality** – obligations to keep your information confidential
8. **Termination and exit** – clear steps that will be taken if the relationship ends, such as return of data and content to you within a specified period.

Pillar 4: Respond when a breach occurs

Despite putting in place industry best practice security measures, there is still a risk of a breach occurring. It is at this stage that the hard work in building a cybersecurity team and strategy, as outlined in the other parts of this paper, will be put into action. The following timeline is indicative and is based on our experience of supporting clients in breach situations. It will need to be tailored for your organisation.

Phase 1

60 mins

Within the first hour

Initiation of Response

— Initial contact with organisation
— Instruction of IT forensics
— Background briefing
— Project plan creation

Phase 2

24 hrs

12-24 hours

Triage and Reporting

— Appointment of outside counsel 'breach coach'/cyber crash team
— Legal advisers typically perform co-ordination and project management role and maintain privilege in communications
— Crisis management and internal communication protocol
— IT forensics assist with identification of source/leak/compromise
— Geographical identification: location of servers and data subjects
— Analysis of nature of compromised material

Phase 3

48 hrs

24-48 hours

Notification and Mitigation

— Early stage evaluation with recommendations
— Recommendation on notification to relevant government authorities and affected subjects (if appropriate)
— Appointment of PR/external communication strategy
— IT continue to identify source/leak/compromise, provide patches and viable alternatives
— Network critical infrastructure brought back online, where feasible

Phase 4

72 hrs

48-72 hours

Implementation

— Is notification required, practicable, appropriate, proportionate?
— Notification of relevant government authorities (by means instructed by the authorities or other reasonable means) and data subjects (by email if appropriate or by a mail order fulfilment centre)
— PR communications and key staff briefings
— Affected parties may be offered post-breach support, such as:
a) Basic advice on security upgrades, improvements, virus patch
b) Web crawling/monitoring
c) Credit monitoring/identity theft

Phase 5

72+ hrs

Claims defence and Regulatory issues

— Notification of commercial third parties, customers etc
— Liaison with the relevant government authorities
— Defence of third party claims
— Loss adjustment and valuation
— Implementation of IT upgrades/amendments (responsibility for funding/betterment)
— Identification of longer term risks and consequences

Your Checklist

Requirement	✓
Pillar 1: Understand your legal and regulatory obligations	
Have you carried out a review of your organisation's legal and regulatory obligations in relation to data and cybersecurity?	
Did the review cover all business units and jurisdictions in which you operate?	
Did it include a review of the contractual security obligations that you are subject to?	
Pillar 2: Build your strategy	
Have you brought together a team of representatives from across the organisation to take responsibility for cybersecurity strategy?	
Have you developed a "benchmark" and been audited against it, to identify any weaknesses?	
Have you developed and implemented a rectification plan to address any weaknesses?	
Have you considered cyber-insurance?	
Have you communicated the strategy to the business and carried out training?	
Have you tested the strategy?	
Do you have a plan to continue testing the strategy?	
Do you have a plan to keep the strategy under constant review?	
Pillar 3: Manage your partners	
Have you considered your partner's security standards?	
Have you looked at your partner's track record in cybersecurity?	
Are you satisfied that you will have control and visibility over your data and content?	
Is the partner transparent about where it stores data and content?	
Does your partner have a suitable business continuity plan?	
Are there appropriate limitations on how the partner can sub-contract or share your data and content?	
Have you considered what happens on termination?	
Do you have a robust contract in place capturing all of the necessary security and confidentiality requirements?	
Pillar 4: Respond when a breach occurs	
If a breach occurs, have you followed the steps set out in your organisation's incident response plan?	
You can use the five-phase response set out in Pillar 4 as a reference.	

How CMS helps

About CMS

CMS is the world's sixth-largest law firm and a global powerhouse in the media sector. Our international team of specialist lawyers has been exposed to virtually every risk and challenge you face in the media sector and with our long-standing focus on media, we are best placed to deliver innovative solutions through our award-winning disputes, corporate, intellectual property, commercial, data privacy, cybersecurity, employment and tax practices.

How we help

Global threats require a global response.

Our trusted cybersecurity team has market-leading expertise and experience in managing all aspects of cybersecurity. Our team provides 24/7/365 availability and a calm, practical and commercial approach.

Our services cover all aspects of cybersecurity for media companies, including:

— Cybersecurity strategy

— Cybersecurity readiness audits

— Risk analysis

— Privacy audits

— Developing and implementing security policies

— Training and eLearning

— Breach hotline services

— Reputation management

— Corporate investigations

— Breach notifications

— Contract review and development

Contact Us

Contact our team to find out how we can help your organisation with its cybersecurity strategy.

Matt Pollins
Partner
T +65 9648 7800
E matt.pollins@cms-cmno.com

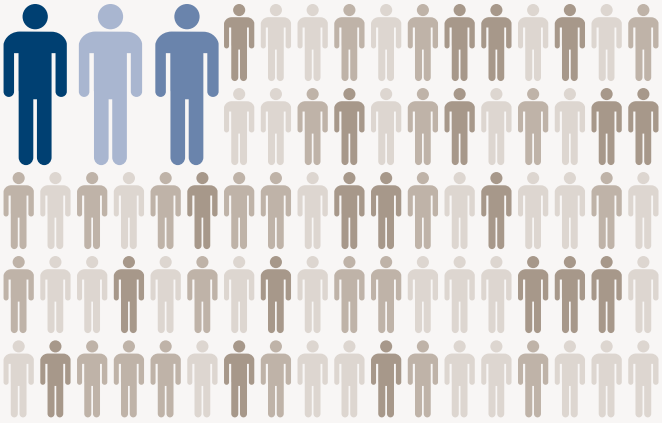
Andrew Stott
Managing Partner - Singapore
T +65 9232 5326
E andrew.stott@cms-cmno.com

Lakshanthi Fernando
Managing Director
T +65 9648 9008
E lakshanthi.fernando@holbornlaw.sg

Jeremy Tan
Director
T +65 6720 8278
E jeremy.tan@holbornlaw.sg

Facts and figures

48 new partners in 2017, taking the total to over 1,000



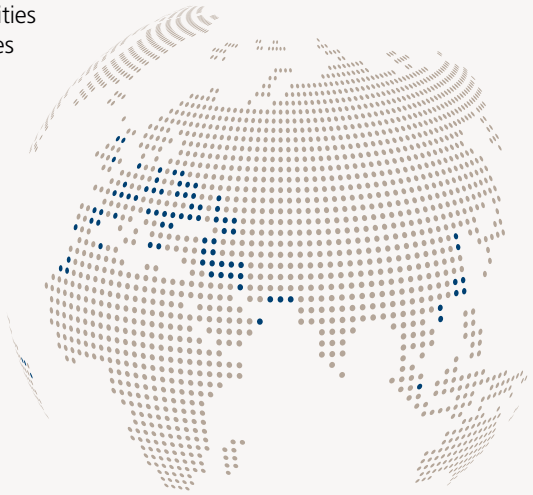
Top rankings in 2016
M&A League Tables (by deal count)

#1 Europe
(Bloomberg)

#3 Global
(Bloomberg up to USD 500m)

Acritas Sharplegal Top 20
Global Brand Ranking

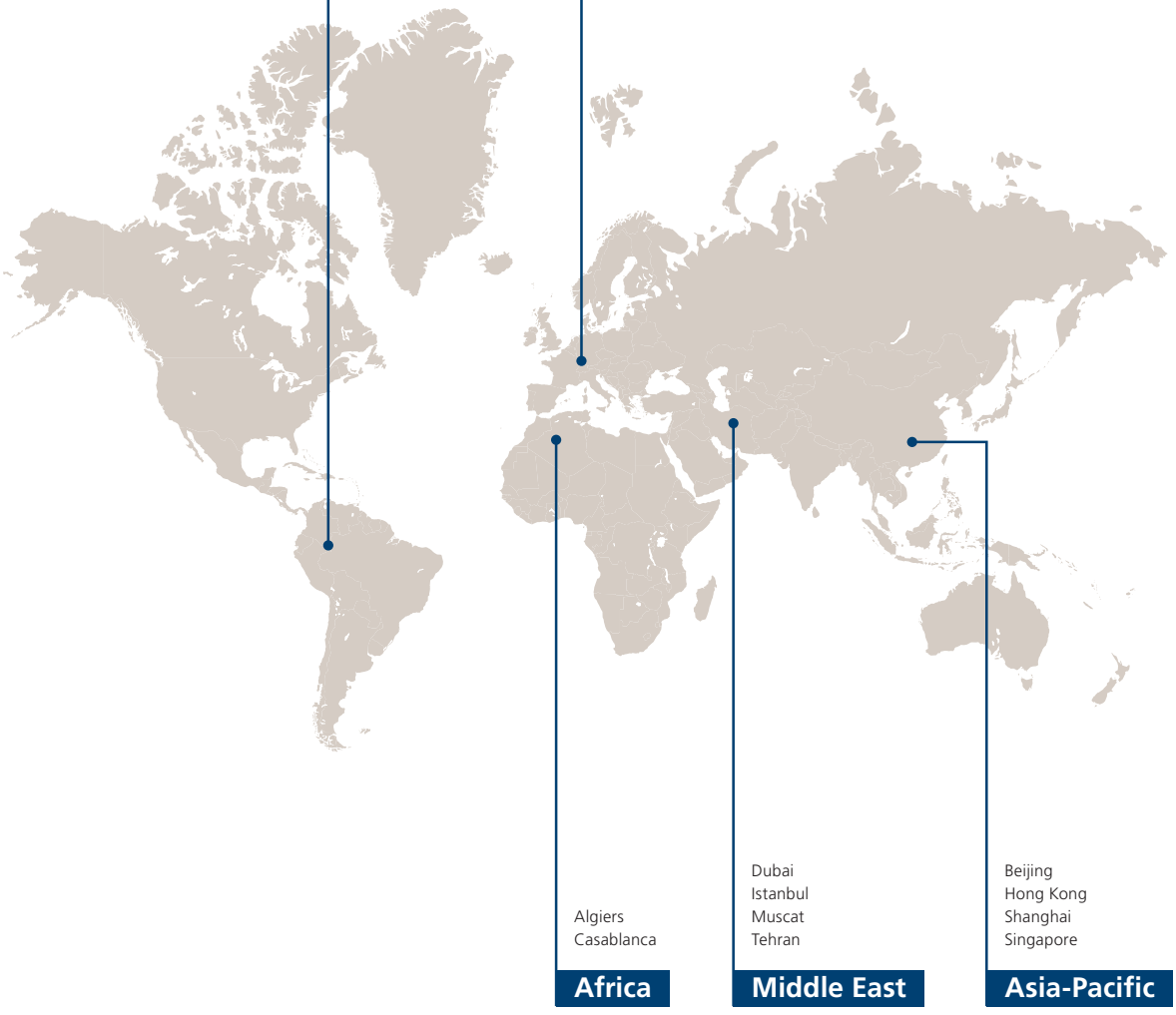
Operating in 65 cities across 40 countries



EUR 1.05bn
turnover for 2016*
* when currency fluctuation is removed

Ranked
3rd
most global law firm in the Am Law 2016 Global Top 100

Where you'll find us – CMS locations worldwide



This paper is intended as a general overview of the subjects featured and does not constitute legal advice. CMS recommends that you obtain legal advice on your cybersecurity strategy.

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1710-0032678-5