American Bar Association
Forum on the Entertainment and Sports Industries
2016 Annual Meeting
October 6-8, 2016 (Las Vegas, NV)

Sports Team General Counsels

Saturday, October 8, 2016
10:45am-12:15pm

Moderator

Glenn Ware
Principal, Leader, Threat Management, Anti-Corruption and Corporate Intelligence Practice Groups, PricewaterhouseCooper (Washington, DC)

Panelists

Ahron Cohen
General Counsel, Arizona Coyotes Hockey Club (Phoenix, AZ)

Nicole Duckett Fricke
General Counsel and Vice President, Los Angeles Clippers (Los Angeles, CA)

Jason Hillman
Vice President and General Counsel, Cleveland Cavaliers (Cleveland, OH)

Caleb Jay
Senior Director, Legal Affairs and Associate General Counsel, Arizona Diamondbacks (Phoenix, AZ)
American Bar Association  
Forum on the Entertainment and Sports Industries  
2016 Annual Meeting  
Las Vegas, NV  

Sports Team General Counsels  
Saturday, October 8, 2016  
10:45am-12:15pm

Table of Contents

Program Description and Learning Objectives

Supplemental Materials:

Current Issues in Digital Management for Corporate General Counsel

Protecting the Franchise: How to Face the Evolving Threat Landscape in Professional Sports  
By Glenn T.Ware and Christopher Sanchez, PwC  
November 2015

Strong Athletic Compliance Programs: A Win-Win for Athletic Departments and Universities  
July 2015

Managing Threats and Maximizing Opportunities for High Visibility Sporting Events
What is a General Counsel in terms of business versus traditional legal skills and roles? Most GCs will tell you they are business people with a legal background. In professional sports, business skills are especially relevant to a GC’s success but exactly what does that mean? Join our panel of legal sports professionals who will help you gain a better understanding of the scope of sports law and uncover the specific unique traits that set a sports General Counsel apart from traditional corporate lawyers.
Current Issues in Digital Management for Corporate General Counsel
Without a doubt, the “digital revolution” has improved the lives of millions of people all over the globe. Driven by the Internet, digitization has enhanced transportation, communications, healthcare, personal safety, the environment and countless other areas of our lives. Global sourcing and supply chains, disaggregated business models, cloud and mobility technologies have delivered the promise of efficiency and the consequence of security vulnerabilities. The “Internet of Things” has begun to take shape in both consumer and industrial markets. From automobiles to appliances, healthcare diagnostic equipment to electric metering, everyday objects that surround us are now arriving with built-in sensors that connect with the internet and large corporate networks.

Many companies that are involved in the digital economy, however, face a significant and largely unappreciated problem: they don’t realize the depth and breadth of their digital exposure. They don’t fully understand that sophisticated threat actors have the means and motives to gain access to valuable corporate data and intellectual property. Realistically, without an informed understanding of the constellation of external and internal threat actors, their goals and their ways of operating, companies cannot identify their systemic weaknesses or effectively manage the genuine risk.

Look beneath the covers at many companies and one finds a technology environment and governance model that lags the company’s obligations for operating in or producing products for the digital marketplace. The data on sources of known data breaches suggests that the prevailing corporate mantra of “doing more with less” is problematic as applied to technology budget cuts. Adversaries calculatingly capitalize on the deferred maintenance, failure to upgrade hardware, sporadic security patching, over reliance on outsourced skills, employees bringing their own devices to work, and lack of monitoring of corporate digital devices to gain unauthorized access to highly sensitive information, including trade secrets, at many companies.

For the US, the government estimate for industry losses due to intellectual property theft alone is $300B annually,¹ not to mention the additional costs associated with identity theft, money laundering, fraud, and economic espionage. A recent private sector study conducted by PwC and CREATe.org estimates that the value of trade secret theft ranges from one to three percent of the gross domestic product of the US and other advanced industrial economies.² 25% of participants in the PwC 2014 Global Economic Crime Survey reported experience with cybercrime, resulting in known losses of over $1 million for 11% of that participant group.

Adding further complexity and cost, regulators and courts have started to get involved—in meaningful ways. The appreciation for the damage caused by privacy breaches in the European Union (EU) has recently become even more acute. Data protection authorities there initially proposed penalties of 2% of global revenue for companies with future breaches, and the cost and

compliance impact on global companies of these regulations (now under discussion within the EU) could be substantial.

In the US regulatory arena, the response has been more measured, but is increasing in pace and scope of coverage. In late 2011, for example, the SEC provided guidance for the voluntary disclosure of cyber risks and breaches. In early 2013, in response to the Senate’s failure to pass a comprehensive cybersecurity bill, the White House issued an Executive Order to establish cybersecurity standards by industries within a “critical infrastructure” framework. Additionally, cases in the U.S. courts suggest judges are now reconsidering the enforceability of certain “boilerplate” exculpatory language in business contracts when one party does not properly secure its business infrastructure—resulting in damages. Increasingly, the various branches of governments are adding teeth to the proposition that the privilege of enabling digital commerce comes with an obligation to protect select elements and aspects of that exchange. Corporate General Counsel (“GCs”) are necessarily devoting substantial time and resources in reacting to the varied and complex legal and regulatory issues resulting from a fast-moving digital marketplace.

I. Issues and excuses—how have we arrived at this situation?

How did we get here? A variety of factors contribute to problem—some within and some admittedly outside the control of GCs and corporate management. The rapid pace of technological change\(^3\) has made it difficult to anticipate the direction or components of digital evolution. Fast-paced information technology innovation and shortened product life cycles have presented management, data security and operational challenges for corporations of all sizes—e.g. whether and how to keep up, how to maintain existing systems, and how to integrate the new technologies with legacy systems.

Another tough obstacle is the issue of SEC period-driven reporting priorities. The U.S. public markets construct encourages shorter term, three-month period by three-month period corporate prioritization and provides little incentive for thoughtfully taking the long view of evolving complex corporate issues such as data security.

Well within the realm of corporate managements’ control is the basic, much-overlooked and increasingly important issue of digital governance—who has the responsibility to manage the company’s digital opportunities and risks, and the related management costs?

\(^3\) “Technological breakthroughs” is one of the 5 PwC megatrends identified in its recent publication “Building trust in a time of change” Global Annual Review 2013 (PwC Review)
Generally, in the absence of clearly defined responsibility, corporate decision-making tends to be ad hoc and circumstantially-driven. Inaccurate assumptions are often made about who is responsible for what. The result is that potentially significant issues can fall through the cracks. It is therefore no surprise that in the vast majority of companies where there is no single point of responsibility for digital management, data-related issues have not received the appropriate level of attention because of inadequately informed and/or empowered personnel. We have seen this on many occasions, where a breach incident has been facilitated by ambiguous internal responsibility for identifying and mitigating fairly obvious system vulnerabilities.

These issues are obvious when a data breach of personal identifiable information (PII) happens and third parties need to be notified. It is at this point that the corporate management’s often limited view of breach incident consequences gets exposed, as the costs of remediation extend beyond technical fixes. Repercussions may include: notifying regulators (requiring outside professional assistance), possible fines and penalties, unwelcome negative media attention and reputational loss.

It is also at this less than optimal stage that GCs must deal with the consequences, and are called upon to lead legal and regulatory consequence mitigation and remediation efforts.

Moreover, conditions are ripe for digital-conduct related negligence to materialize in the corporate liability landscape for the following reasons:

A. An increasingly sophisticated and informed data-consuming buyer: The digital market is highly competitive on price and features thanks to a huge, discriminating and demanding buyer sector. Corporations are digitizing product and service offerings at an unprecedented level. The mainstream and web-based media closely follow digital offerings, and are quick to highlight corporate digital missteps and the implications for individual privacy and other rights. Influential regulators and judges are part of the digital buying public, of course, and similarly rely on digital products and services in their personal and professional lives.

B. The often overly broad claims of digital service and products: A number of companies continue to make exaggerated or baseless advertising claims about their products’ or services’ usefulness, capabilities, reliability and security to obtain market share in crowded and competitive markets. Words like “secure,” “trusted” and “reliable” are seemingly used indiscriminately, and without consideration of their possible legal meaning, impact and consequences. Terms such as “always on” and “tested by the leading experts” can create expectations and reliance— with attendant damages claims if those claims are not met.

C. Growing systems complexity in a continuously lean budget environment: The complexity of managing large digital environments continues to increase, even as corporate IT budgets face continued pressure to cut costs and ‘do more with less.’ In this situation, among the first areas to receive a cost cut is maintenance of legacy infrastructure components (often with latent security and other operational issues, but still important as repositories of critical historical data and/or as the means by which critical reports are generated.) The result, effectively, is a level of enterprise technical debt where delayed attention to existing technical issues results in increasing costs over time and off-balance sheet liabilities that may not be discussed by management.
Current issues in digital management for corporate general counsel

or raised to external directors. Even as the complexity and associated risk of the digitization of global commerce increase, corporate digital security expenditure and effort are not generally keeping pace.

D. An evolving (and increasingly digital consumer-oriented) legal and regulatory environment: Data protection has been the primary focus of US regulatory activity to date, at both the federal and state levels, as disclosure requirements and financial penalties, among other tools, have been used to protect PII, particularly in the financial services and healthcare sectors. At the federal level, certain cyber risks have received direct attention in the form of the SEC Disclosure Guidance issued in 2011, and indirect coverage through the FAR certification in cost plus contracts on “adequate accounting systems.” In 2013, the SEC began reviewing whether greater cyber-attack disclosure obligations should be placed on public companies, as SEC Chair Mary Jo White responded to the strong interest of Senate Commerce Committee Chair Jay Rockefeller and others in enhanced cybersecurity measures for U.S. industry. Additionally, the proposed Cyber Intelligence Sharing and Protection Act (CISPA), now under consideration by the Senate, emphasizes a voluntary collective public/private sharing of cyberthreat and cybersecurity system information, and the present House version is quite similar. More recently, however, there have been potentially significant digitally-related developments in the U.S. courts as various appeals courts have begun to deny procedural motions to dismiss based on technicalities, and are sending cases back to the trial courts for rulings on the merits. As such, cyber-related case law will begin emerging. Arguments concerning negligence or failure to apply commercially reasonable digital security procedures will be tested and ruled upon.

To summarize the current state of the legal and regulatory environment in the U.S.—we appear to be at one of these historical inflection points. After decades of rapid technological change with relatively little accompanying legal or regulatory movement, meaningful societal boundaries are beginning to take shape. In the next few years, we should expect continued and expanded attention to digital regulation, and creative and possibly disruptive litigation around digital rights and responsibilities in our court system.

Similarly, we should expect overseas jurisdictions to generate more guidance with respect to digital behavior within their respective legal and regulatory frameworks—given the pervasive influence of the digital economy on a global basis. The European Union is in the process of making its already strict data protection coverage even stricter and more detailed, and passage of its Regulation (the data protection framework) and the Directive (covering personal data protection) could take place during 2015. If the proposed changes take effect, any business with European customers will need to comply through implementation of detailed compliance policies and procedures, to include, in certain instances, prompt data breach disclosure to affected parties, audits, appointments of a Data Protection Officer and other measures involving additional resources and management attention. Europe’s already strong interest in data privacy for its citizens was further spurred by the recent allegations of surveillance of European citizens by US intelligence.


agencies. Various Latin American and Asian countries are considering a range of approaches to data residency, breach disclosure and other related digital topics.

E. Lastly, but still significant and influential, are the various US digital standards that are emerging, particularly with respect to cybersecurity. For example, the President’s February 19, 2013 Executive Order 13636—Improving Critical Infrastructure Cybersecurity, and the more recent U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) October 23, 2013 Preliminary Cybersecurity Framework are, for the first time, laying out a voluntary national digital security framework, and offering related methodologies and desired profiles. If the large digital industry participants embrace the NIST standard, it effectively becomes the bar. Other serious market participants may need to meet or exceed those strategic and operational criteria to compete. It is also possible that aspects of NIST may become the de facto measure for the standard of care in future digital negligence cases. Accordingly, even though these voluntary standards are not ‘hard’ in the sense that they are required by law or regulation at present, characterizing them as ‘soft’ is misleading because of their potential to exert real power in the marketplace.

II. The needed response—and possible forms of that response

To help prepare for and help avoid or mitigate the potential costs involved, GCs may want to consider certain proactive steps.

A. Analyze and elevate communications about significant digital topics

Ask yourself: Are non-IT and IT executives communicating openly and honestly with each other about the company’s digital risks and opportunities?

We’ve observed that sometimes, and particularly at crucial times, each views the other as a threat, and that therefore communication about important digital topics does not take place at an acceptable level of depth. Specifically, during budget or even operational planning, non-IT senior management often views the IT department as the proverbial ‘black hole’—where vast and disproportionate quantities of money disappear, with seemingly little to show for it, and therefore makes arbitrary, albeit IT-impactful, decisions. On the flipside, IT management, for its part, often views the other group as out of touch with digital realities—especially in the area of security—and ill-informed. Since budget cuts or operational changes affecting IT appear inevitable, they absorb them often without communicating or documenting the consequences.

Both views miss the point—and are essentially a function of not fully understanding, or being inclined to take the time to fully understand the others’ point of view. Because non-IT management may not be given the technical debt or impact information, this group doesn’t understand the depth and breadth of the company’s IT weaknesses and vulnerabilities, specifically with respect to its overall systems integrity and data protection capabilities. And because IT management is often faced with the non-negotiable ‘do more with less’ predicament, this group may understandably focus on the optimally prudent new or enhanced services that result in reward and recognition for the department.

Furthermore, because critical facts or possible scenarios may not be openly and honestly discussed, other functions, such as the GC, for example, cannot add the value that they might otherwise provide.

To help remedy this situation, and to remain competitive in a digitally-based global economy:

- Have IT or an independent third party conduct a corporate digital risk and technical debt assessment focusing both on the company’s systems and the data (its own and third parties’) within its possession or control—and present same to management;
- Have the legal department conduct a holistic (to include legal risk areas that a breach could introduce) and thorough potential liability assessment—focusing on the findings of the assessment—and present same to management;
- Have a cross functional team identify and catalogue the company’s digital assets (to include its intellectual property),
and provide recommendations on increasing the benefits and uses of this often under-appreciated asset base—and present same to management; and

- Conduct a Board presentation—with leaders of each of these respective activities presenting summary findings to the board, along with a presentation of senior management’s overall corporate digital management strategy. These activities, if conducted on a reasonably transparent basis within the company, should help with making communications about difficult digital subjects more honest and open.

B. Establish Appropriate Corporate Digital Governance

Governance is a key component of any company’s digital strategy—and one that is singularly lacking, in a real sense, in most companies. Who has the responsibility for managing the company’s threats and opportunities? What is the scope of that responsibility—what does it include and what does it exclude? Within that scope, does the person have the requisite training and experience to be effective—and to quantitatively and qualitatively analyze the various strategic, operational and technical aspects of the company’s digital past, present and future? What other significant corporate responsibilities does this person have that might interfere with or prevent the digital management function from getting the appropriate amount of time?

Too often we have worked with GCs (functioning as the de facto risk executive charged with cleaning up a crisis) and witnessed situations where companies are forced to address questions of this type from a defensive posture—where the absence of a single and qualified point of responsibility becomes obvious to regulators in the course of investigating a data breach.

The fact pattern that often emerges is that the CFO was nominally in charge of IT, but he or she was not able to effectively assess the business risks in order to make prudent business decisions. In other situations, we’ve found that executive responsibility for the IT function was disbursed among several persons—and that, in the absence of the ownership that comes from a single point of responsibility—significant digital governance issues simply fell between the proverbial cracks.

Functional departments often contract with third party providers without the knowledge of IT. As a result, safeguards are rarely properly applied. Product Development works beyond enterprise network protocols potentially creating unanticipated product liabilities. In these situations, it often comes to light that the board did not receive periodic reports from any member of management on potential digital issues or any related mitigation or response strategies. This is not a situation that any company wants to find itself in (or that the GC wants to defend), and it may be avoidable with proper attention to the digital governance issue.

C. Leverage Available Tools to Help Prevent and Prepare for Possible Digital Crises

Prudent companies recognize the value of preparing for foreseeable adverse digital incidents. There are a variety of tactical steps that a company can take with little additional cost or undue effort to help enhance its digital incident preparedness. Consider:

- Risk Registers: Many US companies have corporate risk registers generated as part of an enterprise risk management program, as part of a risk assessment exercise and/or for purposes of listing and analyzing risks for SEC reporting purposes. If such a list exists, critically review it for possible
updating or elaboration in connection with a more detailed treatment of digital risks.

- **Business continuity/specific incident response planning:** Responding to the disruption caused by Hurricane Sandy in the Northeast, the SEC recently issued staff guidance on business continuity planning for financial services companies. In time, this guidance could be expanded to include other business sectors and/or become an actual disclosure company covering whether or not, and if so, to what degree a registrant had such a plan in place. Table-top exercises can test the adequacy of business continuity and incident response plans, and a corporate team’s response to the given challenge. There is no substitute for ‘trial by fire’ and these simulated exercises have proven to be helpful to identify and improve responses to the expected and unexpected communications, governance, logistical and other issues that inevitably arise in a crisis.

- **Internal audit assessments:** A knowledgeable and well-trained internal audit team can help add value through initial and subsequent audits of various aspects of the corporate digital threat and opportunity landscape. Internal auditors should look beyond the general computer controls for financial system reporting and into the reasonable controls required of the company for operating in the digital domain. If necessary, independent third party experts can supplement or provide subject matter assistance to the internal audit team.

The costs associated with using the above tools can be minimal, and are insignificant by comparison to the costs associated with any material adverse digital incident.

D. Capitalize Upon The Strategic Opportunities Associated With The Technical Debt and Digital Governance Issues

Even as the potential adverse impact of technical debt and digital governance issues becomes recognized by companies, management should also consider the associated opportunities. Competitive advantage may come from addressing these issues; the results are less vulnerable IT systems, less reactive demand on financial and human resources to handle the inevitable periodic system “patches” that are required, and an organization with a more realistic and transparent view of its true digital costs and priorities.

As the organization changes and evolves, there may be additional strategic opportunities. In an M&A context, an acquiror may want to add additional due diligence focused on the target’s technical debt—both from the assumed liability and price of the deal/costs to integrate perspectives. In a potential joint venture, there may be more leverage of various kinds for the company having the least vulnerable, better managed IT systems. In a competitive situation, where a company is bidding with others on a sizeable piece of business, that company may wish to emphasize its internal digital priorities, to include its handling of technical debt, as a distinct differentiator.
Sophisticated private and state-sponsored actors are targeting successful companies on a global basis. They are systematically identifying IT weaknesses and illicitly obtaining intellectual property, moving funds and otherwise engaging in illegal and costly acts. The chances of becoming directly or indirectly involved in a digital incident continue to increase, largely because of three factors. First, certain state actors, as well as commercial competitors, have strong incentives to obtain technology from Western companies—with little real risk of specific attribution or commercial reprisal. Secondly, many companies continue to essentially ‘leave the door open’ to such intrusions through their technical debt and digital governance weaknesses. And lastly, there is the human factor: disgruntled or bribed present or former employees (“insiders”) pose a particularly significant threat, as their knowledge of company systems and practices affords them better access to potentially vulnerable data. 31% of respondents to the PwC/CIO/CSO Global State of Information Security Survey 2014 estimated that their current employees were the likely source of digital incidents.

It is therefore prudent to address certain admittedly difficult digital issues on your own terms and on your own schedule, sooner rather than later. The costs may be greater, the stakes may be higher, and the circumstances may be less favorable if it is regulators or the chair of the company’s audit committee asking the tough questions, in response to an incident. The GC can play a meaningful role in this process by emphasizing the importance of dealing with these issues on an internal basis, and on terms acceptable to management, rather than having regulators or other third parties involved in a dispute context.

Here’s a list of questions that can help GCs get started on being better prepared to rapidly respond to an incident:

- Is there an understanding of the technical debt and its consequences in the company, particularly at the senior management level?
- What is your company’s threat surface, and what are its vulnerabilities?
- Has the company otherwise identified and prepared for various possible digital crises that could impact the company and its operations, and have those plans been formalized and tested?
- What duties may exist to which parties in the event of a digital breach or event at the company, and what is the possible range of costs involved?
- Has the company decentralized IT governance or simply decentralized IT spending?
- Who is the single company officer responsible for the company’s management of its digital rights and responsibilities?

Notwithstanding all the positives associated with the ‘digital revolution,’ it is now time for companies and their GCs to step back and objectively assess the aftermath of the last 20 years’ rapid technological change and innovation. For many companies, there is work to be done on the issues of technical debt and digital governance before moving further and faster down the path of digital transformation.
To have a deeper conversation about how this subject may affect your business, please contact:

Charles E. Beard  
Advisory Principal  
PricewaterhouseCoopers  
703 918 3318  
charles.e.beard@us.pwc.com

Sean Joyce  
Advisory Principal  
PricewaterhouseCoopers  
703 918 3528  
sean.joyce@us.pwc.com

Worth D. MacMurray  
Advisory Director  
PricewaterhouseCoopers  
703 918 3313  
worth.macmurray@us.pwc.com
When it comes to business threats, sports franchises and their leagues face many of the same issues as large corporations: they’re vulnerable to a host of both external and internal threats. One difference is the degree to which athlete talent, and risk management around that talent or athlete, is critical to business outcomes. Strategies surrounding talent evaluation and risk management are at the heart of why the stakes in professional sports are so high, and why the industry is constantly under such scrutiny.

It’s not only the tremendous cost of make-or-break talent. Professional athletes and coaches are among the most widely recognized individuals in the world. In a 24/7 media ecosystem, the attention that accompanies any incident involving a top team or professional player — be it on the field or off — can be instantaneous and overwhelming in the impact it has on a team’s brand.

The threats major sports organizations face run the gamut from cyber-attacks to player scandals to physical security threats — all of which can have a significant reputational and financial effect on players, teams, and leagues. One way of addressing these threats is to deploy a specialized form of corporate intelligence called Sports Intelligence. Sports Intelligence solutions are highly adaptable — and extremely well suited to respond to the unique risks facing major sports organizations.

The game is changing: Responding to an evolving threat landscape

In sports, every organization must follow the same rules, and each team largely has access to the same baseline data when it comes to talent evaluation. So how do you gain a competitive edge? More than ever, teams are seeking innovative ways to measure and acquire the best talent — and to carefully manage the risks that often accompany raw talent.

Today, virtually every major sports organization uses sophisticated technology — be it predictive data analytics, risk metrics and/or social media monitoring (just to name a few) — in order to find that competitive edge and protect it, with varying degrees of success. However, these same tools that teams rely on in the hopes of finding an advantage over their peer competitors can also expose them up to new threats should they not implement the necessary corresponding safeguards to protect their assets.

In an industry largely built on handshakes, longstanding relationships and insights, incidents such as the 2015 data breach involving two professional baseball teams should be a wakeup call to professional sports organizations. It serves as a reminder of what can happen if teams don’t continually invest in confronting the evolving threat landscape facing the industry. Beyond cyber-threats, the sheer scale of security risks surrounding sporting events requires teams to conduct sophisticated vulnerability assessments appropriate for responding to the latest threats. Threat actors continually innovate in their methods for attack and intrusion; professional sports organizations must do the same in their responses.
Teams need a fresh perspective when it comes to strategic operations and technologies aimed at combatting this unfolding world of threats. Espionage, cyber hacking, malicious insiders and intellectual property loss have long been hot topics in other industries. It’s time for professional sports organizations to re-assess the way in which they secure their assets and strategically protect themselves.

Players: A more holistic approach to talent evaluation

That potential draft pick, free agent, trade candidate or recruit you’re about to sign looks fantastic on paper, and social media is buzzing with his on-the-field exploits. They pass the so-called “eye test.” But how well do you know the player’s history — or understand the off-the-field risk the player may pose to your franchise and brand? With much of a team’s success in the hands of a few key players, sophisticated risk management is a key competitive differentiator and a crucial component of building a winning franchise.

Leading organizations are integrating traditional on-field scouting reports and game film with Sports Intelligence solutions as part of an effort to create a more holistic picture of the risk/value proposition players represent. Sports Intelligence solutions are aimed at assisting teams in understanding players holistically, expanding beyond traditional on-the-field scouting. Player risk assessments assess non-traditional risk metrics including asset tracing, network/relationship mapping, litigation history and social media analysis.

Talent evaluation and acquisition will continue to be the driving force motivating professional sports organizations. Maintaining a pulse on what players, staff and fans are saying through social media outlets can help you stay ahead of the curve — aware of potential threats to your team and venues, in tune with external chatter on key decisions and able to spot potential player infractions early in order to address them before they become a crisis.
In our real-time media culture, players are turning to social media more and more to communicate everything from what they had for breakfast to potentially concerning comments that may be indicative of larger risk factors. This may include suggestions of drug and substance abuse, performance enhancing drugs, derogatory comments or other high-risk lifestyle choices. Understanding what players are saying and doing when they aren’t suited up for your team can help teams better protect themselves against making unwise multi-million dollar investments on players that may not represent your brand properly.

Predictive analytics and biomechanics in sports – once thought to be revolutionary in their nascent stages of development – are now widely accepted as value-added methods for analyzing athlete performance. Some of these tools are reaching a degree of sophistication to where they might help predict risky player behavior by evaluating the correlation between emotional states and on-and off-the-field behavior.

Sports Intelligence goes beyond your players and staff. Applying similar levels of scrutiny of your business partners, suppliers and vendors should be part of a holistic risk management program — one that enables confidence across your organization.

**Teams: Addressing espionage and cyber-threats**

Teams that find success in innovation may also find a target on their backs from competitors aiming to catch up. Playbook pilfering and espionage are nothing new in professional sports — they go back more than a century in most organized sports. In the cyber age, risks are significantly greater given that business-critical data is increasingly housed in digital platforms susceptible to cyber-hacks.

Threats such as corporate espionage, cyber-hacking, malicious insiders and intellectual property loss have long been hot topics in other industries. As internationally recognized brands with millions of dollars in revenue, sports franchises, too, must prioritize cyber-security. That means setting in place adequate safeguards to protect sensitive assets — including financial and trade or draft information — from unauthorized access.

These measures can be as simple as requiring employees to use unique passwords (and to change them frequently), educating them on the value of safeguarding their systems and data and instituting procedures that limit their ability to transmit sensitive information from secure servers. Other simple steps — including setting up multi-factor authentication and conducting security checks such as breach indicator assessments — may materially enhance the security of your digital assets. Even small investments in this space may yield large returns when it comes to protecting digital assets.

Cyber-theft contains risks to both parties — to the team that is victimized, of course, but also the team that is ensnared in the plot. Both parties can suffer reputational and financial blows to their brand. Independent insight into internal incidents and investigations can oftentimes provide clarity and help minimize damage on the road to resolution.
Physical assets: Security, contingency planning and crisis management

The criticality of the physical security of an organization’s facilities cannot be understated. On game day, tens of thousands of people — fans, staff, players and the press — are consolidated in one location. Teams ought to ask themselves the following questions related to physical security:

- How is your organization prepared to identify potential risks to security in advance of an event?
- In what ways are your personnel prepared to respond to a crisis?
- What is your first move in the event of an incident?
- How connected is your security program with local law enforcement?

Again social media comes into play as social networks are often the first place a potential issue or risk bubbles up. It’s also a good place to resolve or escalate warning signs to proper authorities or team security personnel.

Additionally, as more venues seek certification under the Department of Homeland Security’s Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, pre-certification security assessments will also help determine a venue’s preparedness to meet Department of Homeland Security requirements — an added layer of comfort in a high-risk environment.

Assess and Act Decisively

Effective risk management strategies are not a luxury for professional sports organizations – they are a crucial component of building a successful franchise. Ultimately, teams should approach all threat protection as they would game-day activities — as a critical component of franchise success and sustainability.

Analytical methods of evaluating risks – player risk assessments, cyber-security planning and threats to physical security – are the nuts and bolts of gaining a strategic advantage over competitors. But it’s an organization’s ability to act decisively on these strategies — and to protect them vigilantly — that determines whether or not it will gain, lose or expand its advantage in the never-ending competitive race of professional sports.

For a deeper discussion, please contact:

Glenn T. Ware, Esq.
Principal, PwC
703.918.1555
glenn.ware@pwc.com

Christopher J. Sanchez
Director, PwC
540.424.8755
christopher.j.sanchez@pwc.com

Find out more at www.pwc.com/us/forensics
Collegiate athletic departments are increasingly under fire for compliance-related concerns, including allegations of mishandling sexual assault complaints, abusive coaching practices and findings of widespread academic fraud. Such allegations present significant reputational, financial and legal risk for the institutions.

Attention to alleged bad behavior off the field — and to how such allegations are handled — can cause downstream repercussions for recruiting, brand allegiance and fundraising. Perhaps more importantly, these alleged incidents, regardless of size, scope or outcome, detract from a university's ability to focus on its primary objectives: educating young adults and maintaining the institution's integrity for its alumni population and supporters.

Universities can minimize this risk by developing a compliance program with a few essential attributes, as we discuss in this paper.

**A matter of governance — and, increasingly, liability**

Due to the groundswell of attention these issues now receive, managing conduct and promoting integrity within athletic departments are increasingly becoming matters of high-level university governance.

And there are growing efforts to hold universities liable for the failure to provide such governance. For example, a northeastern university recently agreed to pay US$1.225 million to settle the claims of five current and former female students who alleged that the university responded to their reports of sexual assault with indifference.¹ Another university is facing civil litigation for allegedly showing indifference to, and failing to investigate, a sexual assault by a student basketball player.²

Clearly, the need to establish and implement an effective compliance program is no longer limited to the corporate sector. Government enforcement efforts have long since taught the corporate sector to prioritize establishing effective compliance programs. However, this is a new lesson for universities, which only recently began to endure close scrutiny of their compliance programs, especially within their athletic departments.

Given the unique circumstances facing academic institutions, a compliance program should be robust and comprehensive, but sufficiently flexible to address “hot button” issues which are not typically covered under standard legal compliance structures. And, while most universities do have an athletic compliance officer, depending on his or her reporting structure, duties and responsibilities, this position alone likely is not sufficient.


² See e.g., *Ross v. the Univ. of Tulsa*, 4:2014cv00484 (N.D. Okla. Aug. 18, 2014)
When perception becomes reality

Due to the high-profile nature of collegiate athletic programs, universities are vulnerable to public perception — whether justified or not — of mismanaging allegations of misconduct in an effort to protect their athletic programs.

Such behavior is understandable. Strong athletic programs are a critical source of school pride and brand recognition and, accordingly, revenue and alumni support. In some institutions, loyalty to the university’s athletic programs is so intense as to foster a “sports as king” mentality, wherein misconduct, or even potentially criminal behavior, of athletes and coaches are excused — or at least seen to be.

In a recent report, the Association of Governing Boards of Universities and Colleges (AGB) called for university governing boards to exercise greater oversight over intercollegiate athletics. The AGB noted that “powerful interests that benefit financially from big-time sports, as well as fans and booster clubs with emotional investments, can distort the clarity of mind required for effective governance.”

The benefits of a strong compliance program

A strong, customized compliance program can go a long way toward staving off criticisms of mismanagement of damaging allegations and preventing problems from the outset.

Compliance programs are more than just an added layer of red tape. When designed and implemented correctly, these programs can be valuable tools for mitigating risk and creating a compliance-minded culture — one which facilitates the institution’s mission.

A consistent approach to incident response can provide a level of defensibility around the university’s actions. Such an approach can also give university administrators the confidence that they are making appropriate, informed decisions, even in high-pressure situations in which facts may still be murky.

An effective compliance program is also a signal to external parties — regulatory or otherwise — that, regardless of the outcome, the institution has identified, assessed and resolved the incident in good faith through a robust, structured process.

Developing a compliance framework tailored to the athletic program’s needs will also allow the university to address a broader range of conduct-related issues, while simultaneously developing a culture of athletic integrity.

Many universities choose to engage external third parties to help design and implement their compliance programs. Such a choice can enable the institution to continue to focus on its key objectives and expertise while building confidence among stakeholders that the university is serious about governing these issues.

The top three elements of an effective compliance program

An effective, robust compliance program generally is not developed from an “off-the-shelf” model. It must be tailored to the unique needs and circumstances of a given university.

As every allegation, incident, or crisis inevitably will be unique, a compliance program must also be sufficiently flexible to address varying incidents. A flexible framework should encourage incident reporting and contain a structure for managing, escalating and responding to issues and allegations as they arise.

Although the minutiae of programs will vary, universities should keep in mind certain key, overarching principles when developing effective compliance programs:

(1) Independence and objectivity

A compliance program should be developed in a manner that minimizes the appearance of any conflict of interest. This will vary by program, but at a minimum, it should require that investigations involving members of an athletic program — including student-athletes, coaches, and staff — are handled outside of the athletic department. Athletic departments typically do not have the expertise to handle investigations of this nature, and a department’s involvement in investigations is likely to draw questions of objectivity.

Indeed, the Executive Committee of the National Collegiate Athletic Association recently released a handbook passed a resolution on Sexual Violence Prevention and Complaint Resolution. Among other recommendations, it advises that an athletic department

---


must “cooperate with but not manage, direct, control or interfere with college or university investigations into allegations of sexual violence, ensuring that investigations involving student-athletes and athletics department staff are managed in the same manner as all other students and staff on campus.”

Other mechanisms can reinforce adequate independence. For example, a program may mandate that the director of compliance have direct access to the Board of Trustees. In cases involving more severe concerns, or those with the potential to garner greater public attention, engaging third-party investigation and compliance experts can lend additional legitimacy and apparent objectivity to the incident response — as well as demonstrate the importance the university has placed on appropriately addressing the issue.

Swift, objective and consistent action signals that the institution values all students and staff equally and does not bend the rules for student-athletes or coaches. Further, proper management of malfeasance is a sign of institutional integrity and reinforces the message that athletic department revenues do not excuse improper behavior.

(2) Commitment to implementation

Compliance is not just a “check-the-box” exercise. An entire organization — from the Board of Trustees and president, to the high school student about to sign a commitment letter — must know about, understand and engage with a compliance program.

Critical to a successful program is the “tone at the top.” A compliance program on paper is useless without a credible commitment from a university’s governing bodies and senior officials to enforce and follow through with the commitments contained therein. Similarly, even the best designed program is meaningless if university leaders fail to communicate it to the university population.

Hence, in designing a compliance program, a university should establish a mechanism to announce to all stakeholders its intent to implement a program — and enforce its provisions — while explaining the rationale and value behind the program.

Any compliance program should also provide for ongoing dialogue with stakeholders. A reporting line from the director of compliance directly to the Board of Trustees, mandatory training at all levels, and routine program audits also reinforce the commitment to compliance — and reassure stakeholders that a program is functioning.

(3) A clear and safe reporting environment, and a mechanism for escalation

Frequently, an incident draws publicity because the allegations initially went unreported or were unaddressed.

A functioning compliance program must contain effective reporting mechanisms in which students, staff and faculty feel they can report their concerns safely and easily. Students may, for example, fear raising complaints about a popular coach or student-athlete, especially if the complaining students would be required to speak with a university administrator. But an anonymous hotline and/or appointed student ombudsman could provide students with a more comfortable reporting environment. At a minimum, a compliance program should contain an anti-retaliation policy.

Additionally, not every allegation will require a full-fledged investigation; in fact most will not. But a strong and dynamic compliance program will contain mechanisms necessary to:

- Identify red flags
- Establish escalation criteria and protocols
- Provide guidance on when third-party investigators are necessary

These elements will ensure that incidents receive the appropriate level of attention.

Conclusion

When significant incidents at universities — especially ones relating to athletics — play out in public, the institutions can face considerable reputational, financial and even legal exposure.

While a strong athletic compliance program will never eliminate risk, it can reduce the risk and severity of any damage.

Maintaining such a program not only enables universities to abide by the law, it also reinforces fundamental values for the school, students, alumni and financial supporters — while not detracting from the institution’s guiding mission of educating young people and preparing them for the world beyond the campus.
For more information, please contact:

Glenn Ware  
Principal, PwC  
glenn.ware@us.pwc.com  
+1.703.918.1555  
Washington, DC

Katherine Wisniewski  
Manager, PwC  
kate.wisniewski@us.pwc.com  
+1.703.307.0947  
San Francisco, CA

Sarah M. Gragert  
Associate, Latham & Watkins  
sarah.gragert@lw.com  
+1.202.637.3368  
Washington, DC

PwC’s Forensic Services’ team of experienced professionals is dedicated to helping clients meet the challenges caused by fraud allegations, financial crimes and other irregularities. Our portfolio of services includes: financial crime examinations, forensic technology solutions, regulatory compliance reviews, fraud risk management and fraud prevention, and dispute analysis and litigation support.

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham’s Client Alerts can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit http://events.lw.com/reaction/subscriptionpage.html to subscribe to the firm’s global client mailings program.
Managing threats and maximizing opportunities for high visibility sporting events

Major entertainment and sponsored recreational events not only create tremendous business and recreational opportunities for owners, participants and fans, but also present a host of challenges in managing the threat landscape inherent in these events. Professional and college athletes and coaches are among the most widely recognized individuals in the world. News of bullying, financial malfeasance, and scandals can rapidly emerge anywhere and at anytime. Further, the unthinkable emergency—natural disasters, violent acts, and terrorist threats—necessitate contingency planning and recurrent exercises. Concern for the protection of proprietary franchise information and personally identifiable information is growing. Organisations that proactively address these issues will gain a competitive advantage by mitigating the threats and risks affecting their most valuable assets.

PwC sports intelligence capabilities

- Pre-hire talent diligence, investigations and social media monitoring
- Crisis management
- Advance site security assessment
- Cybersecurity and cyber event response
- Third-party due diligence
- Third-party and counter party diligence
- Forensic investigations
- Game and match fixing, detection and investigation
- Corruption control, detection, prevention and investigations
- Sports event governance

For more information contact:

Glenn Ware  
Principal  
+1 (703) 918-1555  
glenn.ware@us.pwc.com

George Prokop  
Managing Director  
+1(917) 912-7656  
george.w.prokop@us.pwc.com

Sean Joyce  
Principal  
+1 (703) 918-3528  
sean.joyce@us.pwc.com

Christopher Sanchez  
Director  
+1 (713) 356-5642  
christopher.j.sanchez@us.pwc.com

Shane Sims  
Principal  
+1 (703) 918-6219  
shane.sims@us.pwc.com

George Prokop  
Managing Director  
+1(917) 912-7656  
george.w.prokop@us.pwc.com

6-8 months

The amount of time advanced hackers maintain remote access before detection*

171.5m

Estimated total financial impact on university from a sports-related scandal as of Aug 2013**

10m

Estimated minimum financial losses of a professional sports team following the arrest of a player***

407

Number of arrests of US collegiate and professional athletes in 2013****

400 gigabites/sec

Rate of traffic generated by recent DDoS attack,***** the type of attack used by Anonymous against Brazil.

---

* Statistics taken from the 2014 US State of Cybercrime Survey
**** Arrest Nation; Sports Arrest Database for 2013: http://arrestnation.com/2013-arrest-stats/
***** Statistics taken from the 2014 US State of Cybercrime Survey

PwC is Deloitte limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. BS-14-0353-A.0814