Intellectual Property is a Cornerstone of Modern Business

The cost to develop or produce a new pharmaceutical, software operating system or Hollywood blockbuster can average hundreds of millions of dollars or more. Once this first pill or copy has been produced, it can be replicated for pennies. With so much future revenue tied to initial investments in research and development, the protection of intellectual property is critical. However, databases containing valuable information assets are now being systematically targeted by a hacking methodology known as the “Advanced Persistent Threat” (APT).

APTs are a particularly dangerous variant of computer hacking. ‘Black hats’ target individual organizations for an extended period of time and seek to map out internal networks, create trapdoors for later exploitation, and pilfer sensitive information and intellectual property. These predators are patient, deliberate, and often have access to substantial resources. Furthermore, the most dangerous black hats are offshore, out of the reach of federal authorities.

The Perpetrators of APTs Fall into a Number of Categories

Organized criminal gangs: Many are financed by the Russian Mafia and operate out of former Soviet states of Ukraine, Latvia and Estonia. These criminal enterprises are primarily motivated by money, looking to burrow into foreign corporate networks to steal credit card data and other sensitive

Continued next page
A devastating computer virus may have set Iran’s nuclear development back by years.
— news item

There is a great deal of information to suggest that hacking U.S. corporate systems is tolerated if not sanctioned by the governments of China and Russia…”

Politically motivated actors: In 2010, the devastating “Stuxnet” worm attack took a number of Iranian nuclear enrichment facilities offline (see sidebar). Based on the sophistication of the attack and the manner in which the Stuxnet Worm exploited weaknesses in Siemens’ operating software, the attack was the result of years of patient effort targeting the centrifuges at these facilities.

Nation states: These are arguably the most dangerous perpetrators and represent the greatest ongoing threat, responsible for the theft and transfer of billions of dollars in intellectual property annually. There is a great deal of information to suggest that hacking U.S. corporate information for sale in the black market. They are thought to be behind many of the most devastating privacy breach events.

The Stuxnet Worm

In June, 2010, an extremely sophisticated and malicious code dubbed ‘Stuxnet’ was found buried deep in the operating systems of power plants and industrial networks around the world. Able to exploit the hardware and software used to control all manner of industrial systems and machinery, Stuxnet laid dormant until finding its ultimate target: centrifuges used for processing uranium in Iran’s nuclear enrichment facilities. It is estimated that the worm effectively destroyed over 1,000 centrifuges in Iran’s main Natanz facility and resulted in the suspension of Iran’s nuclear materials processing operations. Although there is speculation as to who created the Stuxnet worm, its actual creators remain unknown. It is evident, however, that Stuxnet was developed by a team with millions of dollars at its disposal and with a mission that was purely political.

systems is tolerated if not sanctioned by the governments of China and Russia, with the intellectual property obtained from these attacks shared with companies close to those governments. These attacks focus on research-intensive industries, including aerospace, semiconductor, biotechnology and pharmaceuticals. Companies such as DuPont, Google, Northrop Grumman and Abbott Laboratories have been affected. In 2009 and 2010, energy companies, including Exxon Mobile Corporation, Royal Dutch Shell Plc, ConocoPhillips Inc. and BP plc, had oil exploration data and computerized topographical maps stolen by hackers believed to originate in China.

**What Risk Managers Can Do**

With a mandate to focus on protecting a company’s balance sheet risk against all threats, risk managers are no longer in a position to simply delegate the responsibility for APTs and other network-oriented threats to the Chief Information Officer. Protecting corporate systems by employing the latest data encryption and intrusion protection technology, while necessary, comprises only one element of the layered protection that is required today to protect a corporate electronic information network.

Risk managers would do well to work with their IT, Legal and HR colleagues to:

- ensure business partners, especially those providing critical network infrastructure such as cloud technology, maintain security standards at least on par with their internal requirements and vet them regularly;
- limit insider threats by conducting detailed background checks for new employees, especially those in IT and operations functions, which would identify prior criminal hacking or identity theft activity; and
- obtain appropriate cyber insurance coverage for risk arising out of the theft or loss of customer information or the impact of network downtime as a result of malicious code or a hacking attack.

Technology has significantly increased the risks that organizations face today. With future revenues dependent on the security of data and intellectual property, the need for risk managers to focus on these digital assets is greater than ever.

---

“Tag You’re It”: ERISA “Tagalong” Class Actions and Fiduciary Liability Insurance

By John Minett
Senior Vice President, Claims Counsel
Email: jminett@enduranceservices.com

Contribution by Ray O’Byrne
Senior Vice President, Professional Lines
Email: robyrne@enhinsurance.com

In what could hardly be described as a joyful “Kodak Moment,” Eastman Kodak employees recently filed several putative class actions under the Employee Retirement Income Security Act of 1974 (“ERISA”) in the wake of the company’s bankruptcy filing on January 19, 2012. These ERISA class actions follow years of Kodak’s struggle and their eventual failure to compete in the modern digital era. Kodak’s ERISA class actions are but the most recent examples of suits filed by employees and retirees against corporate Directors and Officers (D&Os) among others, alleging breach of fiduciary duties for permitting their 401(k) and ESOP plans to offer company stock as an investment option.

The first ERISA class actions were filed in the late 1990s and were labeled “tagalongs” because they were typically filed on the heels of higher-profile securities class actions brought in response to a precipitous drop in a company’s share price. Similar to their securities class action siblings, ERISA tagalong claimants allege that the defendants, the “fiduciaries” of their savings plans, made misrepresentations or omissions regarding the company’s financials and/or prospects. Further, they allege various breaches of duties in violation of ERISA, such as the duty of monitoring whether a company’s stock is an appropriate component for its savings plan. In the decade and a half since the first ERISA tagalong claim was filed, class actions have been brought by hundreds of thousands of plan participants who purchased or held company stock during a “Class Period,” resulting in aggregate settlements well in excess of a billion dollars.

Company Stock in 401(k) Plans: A Potential Problem?

Company stock offered as a component of an employer’s 401(k) plan is not expressly prohibited under ERISA, either as a stand-alone investment option or as the company “match.” From a civil liability standpoint, however, the potential for an ERISA class action escalates dramatically any time that a company’s stock is part of the investment choices offered to employees. The corporate meltdowns at
Enron, WorldCom and myriad financial institutions in 2008 resulted in thousands of 401(k) and ESOP employee-participants losing billions of dollars of their savings when their company stock holdings were reduced to worthless assets. Yet even today, as illustrated by the recent demise of once venerable Kodak, company stock still remains a significant percentage of the holdings in millions of workers’ savings plans, particularly those of older employees. Notwithstanding Congress’s efforts to protect plan participants with the enactment of the Sarbanes-Oxley Act of 2002 and the Pension Protection Act of 2006, Congress has yet to prohibit employer-plan sponsors from offering their company’s stock in their plans.

### Fiduciary Duties under ERISA

A “fiduciary” under ERISA is broadly defined as any person (including a legal entity) who exercises discretionary authority or control over the management of a savings plan or disposition of its assets, or has discretionary authority or responsibility in the administration of a savings plan. Fiduciaries can therefore include D&Os, plan administrators, trustees, Human Resources personnel, outside counsel, and investment managers, among others. Fiduciaries must discharge their fiduciary duties solely in the interests of plan participants and must exercise prudence in monitoring and diversifying the portfolio and following the plan documents. ERISA §409 provides that a fiduciary may be held personally liable for losses caused by a fiduciary breach, including a breach committed by a co-fiduciary, if that fiduciary knows of the other’s breach and fails to take corrective action, or such inaction enables the breach.

---

1 Section 3(21)(A) of ERISA.
“Given the record number of corporate bankruptcies in the past few years and prolonged economic challenges, ERISA class actions will undoubtedly continue to be filed at a significant pace.”

divisional D&O policies contain a broad ERISA exclusion. Fiduciary Liability Insurance is underwritten on a “claims-made and reported” basis, and loss/damages (which includes settlements, judgments and defense costs) in connection with a covered claim erode the aggregate limits of the policy, identical to D&O Insurance. Unlike D&O Insurance, however, a Fiduciary insurer typically has the right and duty to defend and to appoint defense counsel.

Underwriters offering Fiduciary Liability Insurance carefully analyze the various plans in place at a prospective insured, considering the sponsor company’s financial condition, stock performance, quality of management, retention of outside experts for investment advice, and ability to successfully manage their business over the long-term. Underwriting of Defined Benefit (“DB”) Plans vs. Defined Contribution (“DC”) Plans involves different risk criteria: for DB plans, underwriters evaluate funding levels, asset diversification, ratio of current employees to total participants-beneficiaries, and investment income projections; for DC plans (which encompass 401(k) and ESOPs), underwriters examine whether there are a sufficient variety of investment options available, administrative fees/expense ratios, and if the DC plan follows the guidelines of ERISA Section 404(c) and other Department of Labor regulations, which can afford some degree of protection to fiduciaries against liability. Limits of liability are generally based on plan asset size and number of plan participants, as well as the factors mentioned above.

Conclusion

Given the record number of corporate bankruptcies in the past few years and prolonged economic challenges, ERISA class actions will undoubtedly continue to be filed at a significant pace. Even when successfully defended through trial, defense costs can easily reach tens of millions of dollars and plan fiduciaries can be held personally liable for breaches of their ERISA defined duties. A Fiduciary Liability Insurance program with adequate limits of liability can provide essential protection for fiduciaries of a company’s savings plans.
After the Subprime Meltdown: The Changing Face of Corporate and Securities Litigation

By Kylie C. McNally
Vice President, Claims Counsel
Email: kmcnally@endurance.bm

As the world of D&O litigation winds down from the explosion of subprime filings and works its way through the mass of multifaceted and complex subprime settlements, a new wave of aggressive plaintiff lawyers are filing lawsuits that are changing the face of corporate and securities litigation. Some of these developments are highlighted below.

Uptick in Follow-on Derivative Litigation

Previously, a 10b-5 stock drop class action suit, alleging fraud or deceit concerning the purchase or sale of securities, would not automatically cause a follow-on derivative suit filing in the absence of a significant accounting issue, restatement or suggestion of a fiduciary breach. In its 2011 securities class action litigation report, economic consulting firm NERA has reported that, prior to 2002, the number of settled cases accompanied by a follow-on derivative action ranged between 11% and 26% per year. This range, however, has skyrocketed to 65% in 2007 and remained above 55% through 2011.¹ This increase in parallel derivative filings significantly adds to the defendant company’s already high litigation costs and threatens to detract attention from or prejudice the defense of the main class action suit.

Multidistrict Litigation on the Rise

Companies now face more multiple suits in different jurisdictions arising out of the same facts and circumstances. While this happened in the past, there is now a noticeable increase in plaintiff-oriented law firms intentionally filing litigation outside the defendant company’s state of incorporation, particularly in connection with shareholder derivative litigation – some would say in an effort to generate fees. This duplicative litigation forces corporate defendants to defend themselves in multiple courts generating much further uncertainty and additional expense.

Merger Suits Automatically Filed

According to Cornerstone Research², merger litigation is now at an all time high. Upon an announcement of a proposed merger, plaintiff law firms now automatically file suit alleging a fiduciary breach, regardless of whether the acquisition is hostile or whether the target company board accepted or rejected the acquisition. Litigation tends to resolve after the deal closes, with defendants typically winning the preliminary injunction which sought to block the deal. Although few M&A suits result in material payouts, this has not stopped plaintiff law firms from filing M&A suits at record numbers, as they still recover enough in fees to make this a profitable part of their law practices.

Companies today continue to face a significant risk of corporate and securities litigation. These new developments, unfortunately, materially add to the already heavy burden and expense associated with that litigation.

² Recent Developments in Shareholder Litigation Involving Mergers and Acquisitions, Cornerstone Research, 2012.
Editorial Board

Emily Canelo, Editor-in-Chief
EVP, Chief Counsel
Endurance Worldwide Insurance & Reinsurance
Email: ecanelo@enduranceservices.com

Catherine A. Kalaydjian, Senior Editor
EVP, Chief Claims Officer
Endurance Specialty Holdings Ltd.
Email: ckalaydjian@endurance.bm

Ellen Erhardt, Production Editor
SVP, Corporate Communications
Endurance Services Limited
Email: eerhardt@enduranceservices.com

Robyn Greene, Production Coordinator
AVP, Corporate Communications
Endurance Services Limited
Email: rgreene@enduranceservices.com

The Edge is a publication of Endurance Specialty Holdings Ltd., a global provider of property and casualty insurance and reinsurance. The Edge is intended to offer current information and opinions on issues facing our valued clients and brokers. If you have any comments, suggestions, or would like to have us address a specific topic in our next issue, please email us at ecanelo@enduranceservices.com or call 212.471.2820.

Executive Management Team

David Cash
Chief Executive Officer
Endurance Specialty Holdings Ltd.

John V. Del Col
General Counsel, Secretary & Executive Vice President, Acquisitions
Endurance Specialty Holdings Ltd.

Michael J. McGuire
Chief Financial Officer
Endurance Specialty Holdings Ltd.

William M. Jewett
President
Endurance Specialty Holdings Ltd.

Joan deLemps
Chief Underwriting Officer
Endurance Services Limited

John L. O’Connor
Chief Administrative Officer
Endurance Services Limited

Michael Angelina
Chief Risk Officer & Chief Actuary
Endurance Specialty Holdings Ltd.

Catherine A. Kalaydjian
Chief Claims Officer
Endurance Specialty Holdings Ltd.

Mark Silverstein
Chief Investment Officer
Endurance Services Limited

Ellen Erhardt, Production Editor
SVP, Corporate Communications
Endurance Services Limited
Email: eerhardt@enduranceservices.com

Robyn Greene, Production Coordinator
AVP, Corporate Communications
Endurance Services Limited
Email: rgreene@enduranceservices.com

www.endurance.bm