

# Treasury's role as the custodian of value for intellectual property and critical information: The impact of operational security on valuation

Received (in revised form): 14th May, 2009

## L. Burke Files

is an international financial investigator for a global firm that specialises in due diligence, asset location and recovery, anti-money laundering and intellectual property. He has investigated hundreds of cases with cumulative losses into the billions. He has written several books and articles on these and related topics.

L. Burke Files, President, POB 27346, Tempe, Arizona 85285, USA  
Tel: +1 (480) 838 1728; Fax: +1 (480) 491 9439; E-mail: lbfiles@lubrinco.com

**Abstract** Intellectual property and critical information (IPCI) have emerged as significant corporate assets, particularly among certain enterprises. On average, goodwill and intangibles represent 75 per cent of a company's value, yet enterprises are losing their IPCI faster than at any time in history due to theft, leaks and inadvertent disclosure. To ensure the company recognises the value of its IPCI, the information must be identified and catalogued in an assets elements registry — a task best suited to the treasury department. Having created such a registry, the IPCI must be protected. As a threat-based management process, operational security (OPSEC) is the most effective tool a company can use to protect its IPCI. Together, the assets elements registry and OPSEC will have a significant impact on the company's value and performance, and will also limit its exposure to liabilities related to assets, value and disclosure issues.

**KEYWORDS:** IPCI, OPSEC, treasury, intellectual property, critical information

## INTRODUCTION

This paper will argue that the emergence of intellectual property and critical information (IPCI) as a significant asset of modern corporations requires thoughtful re-tasking of the treasury department, especially in enterprises highly dependent on IPCI.

The tasks of identification, accounting and protection of IPCI must be addressed to ensure that its value is both utilised and protected. The value of IPCI is an undefined feature in most organisations, however, and undefined problems have an infinite number of solutions — including many that are neat, plausible and wrong. If the firm is to succeed in protecting its assets, the process of identification, inventory, qualification, monitoring and protecting of IPCI requires a coordinated effort

between treasury and the operations, finance, legal and technical divisions. As treasury's role and responsibilities have expanded to include forecasting, internal consulting, compliance, reporting and financial risk management. Treasury is properly positioned to marshal the talent and play the central role in coordinating the creation and maintenance of an IPCI asset elements registry. Some fundamentals are set out below.

IPCI is at the very heart of the modern corporation's vitality. According to a number of studies on business acquisitions and mergers, intangible assets and goodwill represent, on average, 75 per cent of a company's purchase price. Further analysis of this figure finds that intangibles account for approximately 25 per cent 'proprietary technology' and 50 per cent

goodwill. These numbers show, in dramatic fashion, that buyers and sellers clearly assign significant value to intangible assets. This explains why firms around the world are working so hard to protect their IPCI — or so one would think.

The reality is that enterprises are losing their IPCI faster today than at any time in history. IPCI is being stolen, leaked and inadvertently disclosed at a disquieting rate. At the same time, there is alarmingly little effort to define and protect IPCI outside the familiar forms of patents and trade marks.

Why are companies leaking IPCI? The corporate recognition of IPCI is myopic — and the responsibility for protecting IPCI, if recognised, is strewn about the organisational structure without any clearly defined administrator. There is no centralised repository for the IPCI asset elements registry. For IPCI today, the legal department deals with the filings; operations handles the licensing; manufacturing uses IPCI, disclosing it to third parties when its outsourcing process requires it; marketing gives IPCI to ad agencies and creative staff to give them an edge; and sales leaks IPCI to customers when it needs to close the sale.

This is not just the opinion of one man who happens to have investigated many cases of IPCI theft, loss and compromise. The US Federal Government gets it, and is restructuring the law to help combat IPCI theft. The Enforcement of Intellectual Property Rights Act of 2008 became law in October 2008:

‘Key among the legislation’s components are: authorization for the Attorney General to enforce civil copyright laws; enhancements to civil intellectual property laws; enhancements to criminal intellectual property laws; coordination and strategic planning of federal efforts against counterfeiting and piracy; and increased resources for key programs within the Department of Justice to combat intellectual property theft.’<sup>1</sup>

“‘With intellectual property contributing over \$5 trillion to our national economy, it is one of our most valuable assets and we must protect it”,

Specter said.’<sup>2</sup>

“‘The global economy is not working as it should when we buy from countries that have a competitive advantage over us, and they steal from us when we have a competitive advantage over them”, Bayh said. “American businesses lose \$250 billion every year, and we have lost more than 750,000 jobs because of intellectual property theft.”’<sup>3</sup>

Now is the time for modern corporations to restructure if they are going to deal with the very real threats to IPCI being addressed by the US Federal Government.

In the modern corporate world there are few hard and fast rules about who is responsible for what. Responsibility is often divided by functionality. The financial management of a modern company is loosely divided between the offices of the CFO, corporate finance, comptroller, treasury and risk management. In a rigid description, the CFO is primarily responsible for managing strategic risks, planning and oversight of the company’s finances. Corporate finance is closer to operations and is involved with the deployment of assets in a tactical fashion, in support of the strategic plan set forth by the CFO. The comptroller is responsible for the supervision of accounting and reporting within the organisation. Corporate finance is the arm of the company involved most often in mergers and acquisitions and their subsequent integration into the company. The treasury acts as the gears of the corporate machine, where the strategic vision and tactical decisions are put into action items. Treasury thus takes on a role as principal custodian of value for the company. Risk management may or may not be within treasury, but treasury sees the financial risks first-hand and typically deals with both risk and compliance. These roles do not always fit as comfortably as one would like in the modern enterprise. This structure and division took its primary form in the late 1960s, and has evolved little since. What has happened since then is the emergence of IPCI as an asset form, like cash, which can be inventoried,

banked and/or deployed for the benefit of the company.

In designing managerial systems, what makes sense for a construction company may not make sense for a manufacturing company or a high-tech company. 'Form follows function' for architects of buildings, as well as financial systems. The emergence of IPCI as a key form of corporate asset begs a redesign of the modern corporation's financial structure to account for, recognise and deploy IPCI. Corporate vitality will lay within the organisational change that contributes greatest to the development of a robust IPCI asset elements registry.

The balance of this paper covers some areas that will help in the coordination of responsibilities for IPCI within the enterprise, and provide an overview of the information that needs to be managed. This material provides insight to help evaluate the extent to which responsibility for IPCI is fragmented within one's organisation and to address a coordinated solution. It begins with some broad definitions.

## WHAT IS INTELLECTUAL PROPERTY?

Intellectual property is any intangible asset that consists of knowledge or know-how. A tangible asset is physical, it has form, it has a creation date, and its location can be described. Tangible assets are created from intangible assets. While this description is as accurate as it can be in its brevity, it can also describe critical information. So, to be more specific, the definition is redefined below.

Intellectual property is a concept that includes copyrights, trade marks, service marks, patents, trade secrets and other related rights. Intellectual property is an abstraction recognised by the law. The holder of these abstract 'properties' retains certain exclusive legal rights regarding their creation (work, symbol or invention). These rights are specific to the jurisdiction in which they are registered or are covered by international treaties that accept registration in third-country

jurisdictions. Thus, if a legal authority somewhere does not recognise the intellectual property, the holder has no rights. This means that if one's intellectual property finds its way to jurisdictions where it is not protected, this will pose a problem.

In summary, economic properties and attributes that qualify as intellectual property include the following:

- its description should be specific and recognisable;
- it has a legal existence and protection;
- it can be owned and transferred;
- there should be tangible evidence of its existence;
- it has a specific date or event of creation;
- it can be destroyed at a specific date or event.

## WHAT IS CRITICAL INFORMATION?

Critical information is specific information about one's intentions, capabilities and activities, which in the hands of adversaries would allow them to plan and act effectively against one's best interests. It is information about one's company that competitors could use to make it non-competitive, or hammer it into bankruptcy. Identification of a company's critical information should be construed in the broadest of terms and include items such as customers lists, employee handbooks, formulas, shipping and receiving records, travel of key personnel, presentations made at conferences, etc. The following describes a case from Financial Examinations & Evaluations, Inc case files:

It was only a few years ago that a company specifically dedicated to the design and manufacturing of ASIC (Application Specific Integrated Circuits) computer chips was hit with a rash of phone calls to its employees by a recruiter. A very brief and effective investigation led to a security guard as the leak. The guard had faxed the entire employee directory to a competitor. The guard was convinced by a person over the phone to commit this act. The caller identified himself as a vice president of the

company he worked for (who was listed in the directory as well as all of the public filings of the company). The company acted quickly, and with the help of an investigator (us) traced the fax to an e-fax service — they were able to refer us to an e-mail address — the e-mail led us to a public library access point and one private home access point. Within nine days we were on his doorstep introducing ourselves, explaining how we found him and the evidence trail that led us to him. He fully admitted to receiving the information and to reselling the leads to other manufacturers in the semiconductor industry.

Clearly, this company's personnel directory was critical information. It could have been other items such as marketing plans, shipping and receiving logs, expansion plans, layout of factories, design and review of new products, or any other industry-specific information valuable to the competition.

In a company that relies on IPCI, what could be more damaging than having all of the employees who created and manage the IPCI recruited and interviewed by a competitor? The mistake made was that the security guard should never have had access to this type of information. The guard's access to internet, e-mail or fax should have been limited to what was necessary to do his job.

Economic phenomena that qualify as critical information include the following:

- a protected position;
- breadth of appeal;
- competitive edge;
- customer lists;
- discount prices;
- employee directories;
- heritage;
- high profitability;
- lack of regulation;
- lifecycle status;
- liquidity;
- market potential;
- market share;
- marketing plans;
- monopoly position;
- mystique;

- ownership control;
- uniqueness.

### WHY IS IPCI SO IMPORTANT?

IPCI is today's modern economy and the future economy. A crucial point about legal protection of intellectual property is that it turns intangible assets into exclusive property rights — for a period of time. It gives one company the exclusive right to exploit intangible assets to their maximum potential. By turning intangible assets into exclusive assets that can be, if so desired, traded in the marketplace, IPCI protection makes intangible assets a bit more tangible.

If IPCI rights do not legally protect the ideas, designs and brands of the company, then they can be freely used by any other enterprise without limitation — most notably competitors. The company's rights must be claimed, documented and enforced. If not, the firm will have little or no recourse.

However, when rights do protect IPCI, the intangible assets acquire tangible value in the form of property rights which third parties cannot use commercially without appropriate authorisation. While protected assets cannot be used overtly, this does not prevent them from being used secretly. The IPCI still needs to be protected against both inadvertent disclosure and infringement.

### TREASURY'S ROLE AS CUSTODIAN OF IPCI

The company's legal department has been traditionally proffered as a custodian, but this is an off-the-shelf solution and the fit is poor. While the legal department is involved in documenting the origin, as well as in the defence of IPCI, it is not a part of the creation or the commercialisation of IPCI. Furthermore, it is not required to report on changes or impairments to the value of IPCI; it has no background in assembling an inventory of assets and ideas; and it only occasionally and tangentially touches all aspects of the enterprise.

The office of the CFO deals with strategic matters, not with tactical and functional

matters other than as policy and plans. The office of the CFO will probably be the single largest consumer of information from an IPCI asset elements registry.

The comptroller's office supervises accounting, managing payroll and personnel and financial reporting within the organisation. While this is a close fit to what is needed, comptrollers have traditionally been more focused on matters of performance and the bottom line. It is also a position that is a bit outdated, poorly understood, and absent in many companies. This is not to say that these duties are outdated, just that the duties of a comptroller have been divided up and assumed by many of the other financial management positions described here. The fact is that this position is weak or absent in many companies, and the key functions necessary for oversight of IPCI have been primarily assimilated by treasury.

Corporate finance is also not the location for IPCI. Corporate finance is an outward and forward-looking arm of the company. Corporate finance is primarily a consumer rather than a custodian of information. Much like the office of the CFO, the corporate finance department will be consumers of any report on the IPCI asset elements registry.

Treasury is in the best position to coordinate with other departments and deal with issues affecting IPCI value on a daily basis. Other departments are not excluded, as the process must be inclusive, but the home for IPCI and the IPCI asset elements registry is treasury. In this role as custodian for IPCI and the IPCI asset elements report, treasury will be well positioned to give management supporting information on the value of IPCI for matters such as acquisition, licensing, comparisons studies, infringement and sale.

Treasury is thus the logical choice to be the central figure in the commercial life of IPCI. Treasury touches all aspects of the company every day just as cash and IPCI. Further, treasury has certain functional and compliance responsibilities that deal with IPCI, especially if treasury is also dealing with risk management.

Treasury already has responsibility for many of the company's major assets; all that is added is IPCI. If treasury did not have responsibility for the major components of value in the company, how could it follow its organisational responsibilities to act and inform management on assets and workflow or perform its compliance responsibilities? Regular reports on IPCI asset elements — their status, revenue-generating ability and availability — are just as important as reports on cash and cash positions. Making treasury responsible for monitoring IPCI represents a minimal change to treasury's processes — the creation and preparation of an IPCI asset elements registry emulates what treasury already does for tangible assets with intangible assets.

Treasury already plays a key role in reducing losses of corporate cash and assets due to theft and fraud. The process of centralising and monitoring IPCI gives a clear signal to all involved that when a theft, leakage or disclosure of IPCI has occurred, there is a party responsible for addressing the issues. Treasury will assume, along with monitoring, the concurrent responsibility of the leader in loss reduction from theft (infringement) or value impairment (disclosure).

Imagine cash strewn about an organisation without any accounting. Think of cash lying in desk drawers, in employees' pockets, and scattered about shipping and receiving with no central authority to deal with cash inventory. No reasonable person would allow this to occur. This is why companies have controls, audits and reporting standards. Imagine this level of laxity with 75 per cent of an organisation's value and this gives a snapshot of the problem. No other department or corporate function can address this responsibility as well as treasury. It fits like a custom-tailored suit.

## **VALUING IPCI**

Also known as intellectual capital or intellectual property rights, IPCI is recognised as the most important asset in many of the world's largest and most powerful companies. IPCI is the

foundation for the market dominance and continuing profitability of many corporations. IPCI is often the key objective in mergers and acquisitions, and knowledgeable companies are increasingly using licensing routes to extend the life and productivity of these rights all over the world. In evaluating IPCI, one must ask:

- What IPCI is used in the business?
- What is the value of the IPCI (and conversely, the level of risk)?
- Who has rights to the IPCI? (Can the company sue or be sued?)
- How might it be better exploited (eg licensing in or out)?
- At what level does the IPCI risk need to be insured?

Each IPCI asset has its own subcomponent values, but three discrete components need to be broken down for each asset: legal entitlement, legacy brand (or know-how in the case of patents), and exploitation.

Reasons to want or need to value IPCI may include:

- acquisition of underused IPCI;
- balance sheet;
- choice of purpose, ie the purpose of the IPCI and what impact the re-tasking of the purpose of the IPCI will have on its value;
- contribution to a joint venture (JV);
- cost of compromise;
- damages;
- defensive action;
- donation;
- insurance claim;
- licensing;
- obsolescence;
- provenance;
- relief from royalty;
- remainder value;
- retirement;
- sale;
- to establish what to protect;
- transfer.

There are many methods and formulas for

valuing an asset, but they can be summarised in three general categories:

- *cost*: value based upon the cost of the development or purchase;
- *income*: value based upon projected cash flows for a sale, licence or JV;
- *market conditions*: value derived from market transactions, either as a buyer, seller or observer.

### Cost

Here the cost to replace the functionality of the IPCI is estimated. As what is being valued is the process of replacement, one must factor in the existence of current knowledge and more up-to-date information that can eliminate some of the inefficiencies in the process and avoid the costs of previous failed attempts.

The familiar calculation fair market value (FMV) can be summarised as:

$$FMV = \sum_{t=0}^N \frac{FV_t}{(1+i)^t}$$

where FMV is the discounted value of the future cash flows (FV), at any time period in years (t) summed over all time periods. A typical approach to FMV for IPCI, however, can be summarised thus:

$$\text{fair market value} = \text{cost of reproduction/ replacement} - \text{depreciation} - \text{obsolescence}$$

Being less reliant on discounted cash flow, this version is subtly different, and addresses one of many issues unique to IPCI — that the lifecycle of viability and exclusivity may last only a few years or months before obsolescence.

### Income

This is an assessment on what the IPCI can bring the company as a proprietary asset or as a licensed asset. The aim is to calculate the present value of the future economic benefit. Traditional models assume that this income lasts forever, as per the discount cash flow model.

## Market conditions

The value of a sale of comparable property, done at arm's length, in an active, public, fully disclosed market, and done nearly contemporaneously to the valuation. Market value has a severe limitation as there is never an exact match — the process aims to value something that is unique.

When attempting to value IPCI, the following actions should be undertaken:

- state the date of the valuation and the date prepared;
- define the purpose of the valuation;
- define the standard of value (eg fair market);
- define formulas (eg CAPM, WACC, APT, Fama-French, Gordon Growth Model, etc);
- apply a proper discount/capitalisation rate to 'earnings' as defined;
- examine and discuss all common valuation methods;
- include assumptions and limiting conditions, such as
  - company background;
  - economic environment in which the company competes;
  - industry in which the company participates;
  - market in which the company competes;
  - adequately protected 'exclusive' assets for both tangible and intellectual property (operational security is very important);
- obtain a comparative financial analysis with industry performance;
- provide a well-founded definition of 'earnings';
- reconcile values indicated by each valuation method examined;
- select one value;
- disclose sources of information contained in the report;
- disclose assumptions and source of cash flow projections;
- discuss empirical data sources for premiums and discounts applied;
- discuss and analyse guideline companies selected;
- visit the site.

Define and include discounts and premiums such as:

- control and acquisition premium;
- discount for lack of control;
- discounts for lack of liquidity and lack of marketability;
- transfer restrictions;
- risk issues such as regulatory or litigation;
- volatility of market/obsolescence;
- registration/current licensing fees.

Some strategic and tactical things to consider when valuing IPCI:

- *Technology diffused/competing patents*: some technologies are 'me too' ideas that although protected, are protecting different areas of a broad field that has been ploughed many times.
- *Next best thing technology*: there may be pricing pressures when the property is in the process of being superseded by another technology. As an example, consider the case of photography: a decade ago, a reasonable 35-mm SLR camera was usually good for ten years or more while today, many people do not even know what film is.
- *Technology is locked up within national boundaries*: the USA and other countries have restrictions on the export of technology. Further, the mere exportation of the technology may trigger a tax event.
- *Precipitation upon transfer*: IPCI and the companies that control the property often have long histories, and it can be difficult to be up to date with all the agreements signed by past management teams or to be aware of all of the assets, liabilities or restrictions. Some events may be precipitated upon a transfer, such as a bonus, acceleration of a contract for royalties, or fines for a violation of regulatory decrees.
- *Blocking patents or intellectual property*: some technologies are purchased and sold not because of their economic value, but because, through the purchase of a patent,

the owner can block competitors from a market. They are also sold when companies in litigation realise that they may not have full protection, and hope the purchase will improve their position and the case.

- *Not foreign protected*: If intellectual property is not patented in the USA it is not well protected in the USA, and by extension, if it is not patented in China it is not well protected in China.
- *Manufactured documents*: it is not unknown for people who are selling a business to falsify financial statements, licences, documents and even legal opinions.
- *Demand curves (long or short)*: the demand cycle for many products will affect their value. For example, the demand cycle for new memory devices may only be a few years, but the demand cycle for a recognised trade name may be measured in decades.
- *Infringement*: a great number of trade marks and service marks are infringed upon. The values of trade marks are compromised by infringement. If the owner does not mount what is generally recognised as a vigorous defence, the value may be lost.
- *Licence drift*: a licensee is given the right to use the technology in one area, but has drifted into other areas not covered by the licence. This can compromise the value of future licensing opportunities for the owner, and can subject the drifter to damages.
- *Mergers and acquisitions, malaise and panic*: the uncertainty generated during mergers and acquisitions can cause a great deal of angst among those affected. People are anticipating an upset in their lives (for some, any change is an upset) and behave poorly. They may look for work at a competing company, they may sell intellectual property, or in their panicked state may inadvertently disclose IPCI. Situations can arise where one company buys another, only to find that two-thirds of the employees have left within a year, taking with them the knowledge that made the company work.
- *Family-owned businesses*: these businesses often have a cult of personality, and when that

figure is gone, the rest of the gang leaves as well. Family-run businesses usually have a much lower cost structure, because all family members work hard during the day to be able to face one another in their private lives. Such loyalty will rarely survive a sale.

- *IPCI insurance infringement*: IPCI with infringement insurance is more valuable than IPCI without it. Further, if the company lacks the financial ability to defend the IPCI if it is infringed, it could impair future claims against infringement. A claim that cannot be defended is not much of a claim.

## OPERATIONAL SECURITY AND VALUE IMPAIRMENT/ ENHANCEMENT

So far the paper has covered some basic information on the valuation of IPCI. From here, a look at impairments to value is required. Impairments include some factors that have not yet been mentioned and which do not form part of traditional thinking.

The consequences of an IPCI theft are not the actual loss of the asset. As the assets are intangible, one controls them rather than owns them. What is lost in an IPCI theft is the *exclusive* use of the asset. IPCI theft or compromise thus creates instant obsolescence. The following describes an event from Financial Examinations & Evaluations, Inc case files:

Being asked to speak at an industry function is an honor as well as a career boost, so when John had the chance to finally address a conference he had previously only attended, he was delighted. The honorarium was the frosting, and reimbursement of his travel expenses put a smile on his employer's face. That smile might have done a one-eighty had the company CEO known that a chief competitor, the event's secret sponsor, made it all possible. The head of the competitor's company also had a smile on his face: His firm, aggressive practitioners of Competitive Intelligence, had structured the entire conference to manipulate rivals to willingly — if unwittingly — reveal competitive information.

Operational security (OPSEC) is the most effective tool a company can use to protect its IPCI. OPSEC entails the identification, valuation and protection of IPCI from competitive intelligence, economic espionage, casual dissemination and theft. In summary, OPSEC:

- is a management function;
- is threat-based (not rule-based);
- is a process;
- crosses divisions and disciplines (just like treasury);
- helps companies to reduce vulnerabilities to — and therefore derived risk from — competitive intelligence, economic espionage, disclosure and theft of information.

Companies must protect their IPCI, and the logical model for this internal control is OPSEC. This is the accepted US Government standard process for identifying, valuing and protecting information that would give adversaries an advantage. It serves the very same purpose in the private sector — it identifies, values and protects IPCI.

OPSEC addresses five critical questions:

- Who wants your information, and what are they willing to do to get it?
- What information do they want, versus what is important to you?
- Where are the vulnerabilities that would allow competitors to get information?
- What happens if they do get the information?
- What can be done to prevent this from happening?

OPSEC is conceptually simple and initially looks like traditional risk management, but there is a critical difference. OPSEC is a threat-based iterative management process that crosses divisions and disciplines, rather than a rule-based system relegated to one department. When properly approached by an experienced practitioner, OPSEC is highly cost-effective to

implement and maintain, and provides a high return on investment from reduction of losses and decreased liability costs.

OPSEC is a process whereby the owner of IPCI designates what is important and what competitors may want, and devises methods to secure and limit access to that information. Further, there are enhancements to OPSEC that can track stolen IPCI from when it leaves an enterprise all the way to its destination. So how does one know when one has lost IPCI?

### **IMPAIRMENT HAS A 'TELL'**

Poker players call it a 'tell'. Some players have mannerisms that signal the quality of their hand. Some people's voice gets higher when they are bluffing, others tap the table when they have a good hand and are impatient to wager. The loss of IPCI has its own 'tells':

- a competing company is producing goods identical to yours;
- your market share is shrinking;
- other companies can suddenly match your price points;
- there is a sudden and knowledgeable, market pressure on prices.

As discussed, intellectual property does not exist unless it is covered by a legal registration or declaration. Thus, if an item of intellectual property lands in a country where intellectual property is not covered — it is not protected. Say one had a copyrighted book, but that copyright was not registered in Russia or China — then it would not be protected in Russia or China. Further, if a decision is made to patent an item in the USA and the EU but not in China, those patents will not be binding to businesses in China, and an enterprising rival may even file that patent in China and claim it to be their own.

The issue of value impairment is more important following the publication of Financial Accounting Standard (FAS) 141, 'Business Combinations', and FAS 142, 'Goodwill and Other Intangible Assets', which changed the accounting treatment of certain

intangibles during acquisitions. Instead of a more-or-less blanket treatment of acquired intangibles that featured a stated amortisation period, many of these assets will now be carried on the balance sheet at cost and subjected to an annual impairment test. These tests are usually conducted under SAS 81 and or 101 guidelines. The same is true for IFRC 3. All have a significant shift to transparency and impairment tests.

Impairment tests are a step in the right direction, toward providing sane valuations for all, not just public, companies. They represent a good start — but, as demonstrated in many recent failures, valuation rests heavily upon a foundation of subjective assumptions. Information in the balance is released in response to the public's demand for disclosure, and shielded in response to the corporate need for privacy. Treasurers, as a profession, can either take a leading role in the protection of IPCI, or wait for the lawyers and judges with test cases and regulatory fines to dictate responsibilities. Corporate redesign by judicial or legislative *fiat* is a poor alternative to proactive redesign that embraces the value and importance of IPCI.

The lack of OPSEC for a company's IPCI should produce an automatic haircut in the value of any IPCI within the company. The problem is very clear — one (buyer, seller or investor) does not know whether or not the economic advantage proffered by an item of IPCI is exclusive. To put it another way, if you were buying a container of silver bars that was being transported under the utmost levels of security, would you open it to see whether the bars were inside? Of course you would. But that option does not exist with IPCI — IPCI is intangible and is not subject to inspection for verification. Thus, with IPCI one must rely upon the process used to protect the property — and the only acceptable process is OPSEC.

One problem with IPCI is defining theft or loss, as compromised IPCI is still titled to one's company. Competitors are not changing ownership of a thing or an idea — they are simply making use of it. When IPCI is

compromised, what is lost is the right of exclusive use. The rightful owner has lost the right to designate who can make use of their property.

In summary, an OPSEC programme offers the following value enhancement:

- a commercial information programme to monitor competitors both for innovation and for use of the company's IPCI;
- an employment agreement that clearly identifies IPCI and protects it;
- vendor agreements that clearly identify and protect IPCI;
- an IPCI tracking software that can look for IPCI loss 'tells';
- IPCI loss ID and reward programme;
- employee training on the importance of IPCI.

Meanwhile, the lack of OPSEC programme risks the following value impairment:

- no IPCI inventory;
- employment agreements fail to address disclosure of IPCI;
- vendor agreements fail to address disclosure of IPCI;
- lack of information security;
- no programming to identify IPCI as it is created;
- inability to track competing technologies.

## WHY OPSEC IS SO IMPORTANT

According to the US Government,<sup>4</sup> competitive intelligence, economic espionage and intellectual property theft cost US business US\$300bn a year — a figure that represents 2.25 per cent of the country's GDP and which translates to 750,000 jobs needlessly lost each year — and the number is climbing. The estimated average per incident cost for a manufacturer is US\$50m, with non-manufacturing victims getting off relatively easy at only US\$500,000.

The problem is global. *The Korea Times*<sup>5</sup> has suggested that half of South Korea's high-tech companies have suffered from leaks of

proprietary information. Denmark's *Economic Weekly*<sup>6</sup> newsletter says that the number of industrial espionage attacks against Danish businesses is exploding. Other countries report similar findings.

There are a number of factors behind this epidemic:

- Although it is estimated that intangible assets comprise 75 per cent of the value of a modern company, many firms have never itemised their IPCI inventory or its disposition, and have never even considered the economic implications of losing an asset that is off-book. Most do not even know what needs to be protected.
- More enterprises are investing in competitive intelligence programmes, making them active threats to all competitors' IPCI.
- The end of the Cold War saw a shift from military to economic intelligence gathering, of which more than 90 per cent involves legal competitive intelligence techniques.

Although information loss has, by inadvertent neglect, become an invisible and out-of-control cost, few managers show any interest in arresting the losses their companies have probably already suffered and continue to be exposed to. Indeed, the American Management Association once told a colleague that the subject of IPCI theft was of no interest to its members. The lack of interest and concern is not surprising. Schools of business, law and criminal justice discount the dangers of IPCI losses, and spend even less effort teaching countermeasures to avoid losses. The FBI made a post-Cold War commitment to fighting economic espionage, but law enforcement's reactive posture (solving crimes, not preventing them) combined with pressures post September 11th, have removed the agency as a significant preventive force.

The trends are manifestly negative for the unprepared company. Today's labour forces and lifestyles are another growing threat. About 4 million workers in the USA are extreme commuters — people who travel for

90 minutes or more. Most of these people will use this time to work when they can. Who is looking over their shoulder as they use their laptop on trains or aeroplanes? Considering that about 4 million more people work part-time at home, US industry has about 6 per cent of the workforce outside of a 'secure' company location, creating many millions of opportunities for IPCI loss to occur away from a 'secure' facility. Laptops can be stolen when employees leave them on train station benches or with airlines; they can be hacked into through wireless access cards, and gigabytes of data can be transferred to a flash drive in seconds. On top of this, employees are taking their work out of the workplace in an increasing spiral of flexibility to eke every drop of productivity out of the day. Employees are working at libraries, coffee shops, hotel lobbies and parks, all with more and more information on the laptop.

How far can lost IPCI travel? A manufacturer of specialised potions had a unique line of soothing lotions made with a series of proprietary formulas. When a supplier compromised their formulas, a competing product was offered within days, and the first batch shipped within weeks, from 8,000 miles away.

Why do people steal IPCI? William 'Willie' Sutton, when asked why he robbed banks, gave a simple answer — 'Because that's where the money is'. As the owner of IPCI, it is vital to think of its theft as a real crime — something law enforcement is not yet prepared to do. The estimated chance of getting caught stealing virtual property is 1 in 250,000 — the statistical equivalent of losing 18 consecutive passes on a craps table. Of the very few people who are charged and convicted, only one-third face jail time — and of those, 90 per cent are sentenced to under a year. IPCI theft pays.

## **PROTECTING IPCI: WHOSE JOB IS THIS?**

The job of protecting IPCI involves the treasury. The hallmark of the treasury function is to reduce uncertainty through order — as

uncertainty kills finance just as effectively as fraud or over-regulation. ‘Treasurers’, according to James A. Katz, President of the Association of Financial Professionals, ‘are the custodians of value of the modern company. Today’s treasury is no longer just a support division, but is also looked upon as a profit center’.<sup>7</sup>

Management might assume that they are protected by their security and IT departments, corporate counsel, and other outside consultants — but these groups are focused on protecting information *on company property* from *outsiders* and reducing crimes of opportunity. Intellectual losses, on the other hand, are most often the result of trusted people acting *off company property*, whether it is information published by corporate mandate, employees betraying an employer, or talking too freely in an open forum. The following is an example from the case files of Financial Examinations & Evaluations, Inc:

A product sales company was approached by a competitor who wished to buy out one of its stores. To the amazement of the company’s owners, the competitor knew all of the sales of that store for the last three years. It turns out that the landlord of the mall disclosed all of the sales of all of the stores in the mall to any bona-fide prospective tenant.

One should carefully look at all of the third-party agreements for those who have IPCI information under their control. Some examples are landlords, key suppliers, shipping companies, attorneys, accountants, consultants and others. The agreements should provide for no disclosure of IPCI, and what one considers IPCI should be clearly identified. The same is true for employment agreements made directly with employees or with third parties. The agreements should have minimum damages defined, and should be assessed upon the documentation of a disclosure. The agreement needs to be clear and have teeth.

### **Domicile**

The domicile in which an IPCI dispute is

brought is critical. In some states litigation can take years just to see the inside of a courtroom. Many countries lack the intellectual property infrastructure to deal with IPCI matters. Yet some countries do cater to IPCI; in The Netherlands, for example, an intellectual property court has been established where resolution can be sought and resolved in as little as six weeks by people who do nothing but deal with IPCI. It is not just the venue for the dispute that is important; the venue should be a serious concern both in the reading and the drafting of all contracts.

### **Insurance**

Insurance can be purchased from regular line suppliers for litigation, but not for the economic damages resulting from the theft or loss of IPCI. This may be an argument for more creative captive insurance opportunities — but it is not a mainline coverage issue. One must also look at the cost of transferring the risk as opposed to managing the risk of IPCI loss or theft.

### **CONSEQUENCES OF FAILURE**

As most companies pay no attention to the topic, corporate officers face three areas of liability:

- They are technically in non-compliance with Sarbanes-Oxley. This can involve both civil and criminal exposure — and audit firms generally do not know to look for the problem (or where to look).
- If the loss is prosecuted under the Economic Espionage Act of 1996, the perpetrator could make a compelling case that the lack of internal controls, as required by Sarbanes-Oxley, was a failure to take ‘reasonable measures to keep such information secret’. The information would therefore not be a trade secret as defined under the Economic Espionage Act and the model Uniform Trade Secrets Act,<sup>8</sup> making prosecution of the perpetrator impossible.
- Shareholders could undertake negligent action lawsuits claiming managers should

have known there was a high-probability threat that they should have addressed, in addition to having abandoned the trade secret status of information. Because the managers were also non-compliant with Sarbanes-Oxley, the director's and officer's insurance underwriter could claim intentional indifference on the part of management and then refuse to cover the defence expenses, potentially making them personal liabilities.

Although the new legislation did not specifically mandate anything new on the requirement to value IPCI, it did impose greater responsibility on management and significant penalties for failing to protect IPCI. Investors and regulators are paying a lot more attention to IPCI in financials, as shown by the Financial Accounting Standards Board's recent statements on business combinations, goodwill and intangible assets. Recognising how much impact IPCI has on company values, the rule-makers continue to emphasise improved IPCI valuation in financial statements. A first step is to move away from a rules-based approach and to adopt a principles-based approach — a move which requires more professional judgment and less follow-the-dots accounting.

Non-compliance can result in legal as well as survival problems. Think of all the companies in the news whose databases have been compromised, releasing everything from customer data to credit card information. These are the type of stories that make the news, fuelling the public concerns over identity theft. When a US company recently lost the IPCI for making a particular type of synthetic diamond, no one heard a thing.

### **THE IPCI PROTECTION FUNCTION IN THE MODERN COMPANY**

A single department must coordinate responsibility for IPCI valuation and protection. This department would first address intellectual property and assemble all the information on the company's trade marks, service marks, patents, copyrights and trade

secrets. This information should be assembled in a simple database recording the date of creation, costs, challenges and outcomes, as well as any other items thought to be pertinent such as potential offenders or infringements. The database will be a dynamic structure that can be updated as information emerges. Another database will assess critical information for each department, based upon the criteria set forth earlier. Specifically, the critical information database will record all information that the different departments do not want to share with the outside world, especially competitors. The very process of identifying and assembling this information will begin the process of sensitising company employees, letting them know how serious the company has become about IPCI and protecting its rights.

The IPCI asset elements registry should be shared with the offices of the CFO and corporate finance, and its assembly should include the innovators, legal department and the corporate secretary. When reviewing the IPCI asset elements registry, the discussion should identify the locations of potential IPCI leaks (eg to and from third-party vendors, inadvertent disclosures, conferences, as well as other areas of exposure). A review of all agreements should be undertaken to see where disclosures might have occurred, and these should be addressed with addendums. Agreements with employees and outside contractors should be reassessed in light of the company's increased awareness regarding the importance of IPCI, and the non-disclosure language should be reinforced where applicable.

During merger and acquisition activity, the division responsible for IPCI should be involved in assessing the inventory and quality of the other companies' IPCI, and report their findings to the CFO and corporate finance office. If a transaction is consummated, the responsible department should immediately initiate their IPCI valuation and protection measures.

Once the data have been assembled and

actions have been taken to identify and protect IPCI, it is time to consult an OPSEC professional. Prior to an OPSEC audit, prepare a list of competitors who might be likely to target the organisation for information. Typically, an OPSEC professional will perform as a coach, helping to identify vulnerabilities and security flaws as OPSEC procedures specific to the needs of the enterprise are developed.

As a part of the OPSEC procedures and regular reports, the IPCI asset elements registry should be shared with department heads, as well as the CFO and corporate finance in order to maintain awareness and encourage the commercial deployment of these assets. A secondary benefit of the registry is that increased awareness of IPCI often encourages synergistic deployments of IPCI assets that many people in the enterprise may not have known the company possessed.

## CONCLUSION

The industries of developed nations have responded to the theft of IPCI by innovating new technology faster than they leak IPCI. To use a sinking boat as an analogy, this is akin to pumping faster rather than plugging leaks. If the leak is faster than the pump, the boat sinks.

In 2008 there were nearly 500,000 patent applications, and 182,556 issued. Of those issued, 49 per cent were to US companies,

Japan was second with 23 per cent, and Germany was third with 5 per cent. The developed commercial world is investing in IPCI.

The objective is to foster an enterprise with margins that will be protected, that will not leak information, and that will have a far higher market value than its contemporaries.

To reiterate, the only change in the focus of treasury would be to unfold its ledger a bit further to include responsibility for monitoring IPCI. The creation and preparation of an IPCI asset elements registry in many ways mirrors what treasury is currently doing with tangible assets.

As stated previously, treasury is in the best position to coordinate these efforts.

## References

- 1 <http://bayh.senate.gov/news/press/release/?id=fe6b748a-8558-4fd0-c50d88e23b90>, 24th July, 2008, accessed 24th July, 2009.
- 2 *Ibid.*
- 3 Senator Specter's News Release on The Enforcement of Intellectual Property Rights Act of 2008, 24th July, 2008.
- 4 2002 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.
- 5 Jinseo, C. (2006) 'Half of Top Tech Firms Suffer Leaks', *Korea Times*, 19th June.
- 6 Gullev, B. (2006) 'Increased espionage against Danish businesses', *Borsen Online*, 28th August.
- 7 Association for Financial Professionals (AFP) Regional Conference (2007) at Tampa, Florida, held on 8th June.
- 8 The Uniform Trade Secrets Act (UTSA) is a model law, adopted by 46 states, to clarify rights and remedies in cases involving trade secret misappropriation.