THE FIVE SECRETS OF PROTECTING INTELLECTUAL PROPERTY

CSC

How to tackle the insider threat

TO PREVENT INTELLECTUAL PROPERTY THEFT

Tackling the insider threat
TO PREVENT INTELLECTUAL PROPERTY THEFT

Ford Motor Company, DuPont, Dow Chemical, General Motors: they've all had well-publicised incidents of employees or former employees stealing trade secrets. Is there simply nothing to be done to prevent such acts? Is it a 'cost of doing business' for industries such as manufacturing, automotive and pharmaceuticals — industries where hundreds of millions of dollars can ride on specific pieces of intellectual property?

For most of my career I've been deeply involved in protecting highly sensitive and valuable commercial and government information, and there's no doubt in my mind that there's a lot that can be done to minimise the chances of such thefts. But most of it has to do with culture and people and processes, and for most organisations that makes it challenging. They may have set relevant security policies and invested in firewalls, remote access controls, cryptography and such, but none of that defends against the disgruntled, bribed or blackmailed employee.

Security policies on their own aren't enough. And there's no single technology, nor indeed any suite of technologies, that can address the problem of intellectual property theft adequately on its own. There's no doubt that the right information security policies and technologies can and should play an important role — and we'll talk about some of them in this paper — but they're of limited use if not embedded within an enterprise-wide risk management regime encompassing everything from hiring policies to business process design.

The approach offered here need not be expensive – in many circumstances the threat can be met by integrating and co-ordinating work that is already being done. In organisations that are hugely dependent on intellectual property, the real risk is not investing in protecting it.

When CSC explores the needs of the companies that ask us to help them protect their intellectual property, we find that often they're doing some things very well. But prevention of intellectual property theft is a multifaceted issue that requires an integrated approach across many enterprise functions. It's a job for the whole organisation, not just IT, as this paper will show.

In this paper we discuss the five principles that our long experience in this area tells us are fundamental to preventing IP theft. It's quite possible you're already on top of one or more of them; but they all need to be tackled in parallel if you're serious about reducing your IP theft risk.

Nick Hopkinson, General Manager,
Cybersecurity (Europe), at nhopkinson@csc.com

THE FIVE SECRETS OF PROTECTING INTELLECTUAL PROPERTY

1 MANAGE BY FACT

It sounds a bit obvious: clearly you want your actions to be based on fact, not fiction. But it's worth stating because, in reality, most organisations aren't taking the right approach to ensure that they *have* all the facts about the risk of intellectual property theft. And you simply can't be led by the facts if you don't have them.

Here are three common approaches to risk assessment to avoid. These approaches generally won't give your organisation an appropriate understanding of the risks you face in relation to IP theft (or indeed any other risks):

- **DON'T TREAT RISK ASSESSMENT AS A ONCE-OFF OR INFREQUENT ACTIVITY.** Risk assessments need to be done periodically to capture your changing risk profile and embed risk management into the operational culture of your organisation. How frequent this period is depends on the risk you face. In some circumstances, an annual review is appropriate. Others may require the exercise to be done much more regularly.
- **DON'T PERFORM RISK ASSESSMENTS PURELY AS A BOX-TICKING EXERCISE.** This is often done to satisfy compliance requirements — and may even be done regularly. But a narrow and mechanistic approach to risk assessment, however frequently performed, tends to result in important risks being missed, especially as things change in your organisation (which they always do).
- **DON'T PERFORM RISK ASSESSMENTS IN SILOS.** We speak to many organisations that analyse the financial risk of X and the operational risk of Y, but not vice versa. Or they run careful risk assessments for projects but not their day-to-day operations. Or, again, they look at risk too narrowly; for example, the IT department may take a particular view of the risk to a system without fully appreciating how its role in a whole business process exposes it to additional risk. In relation to IP theft, for example, IT may not adequately appreciate the likelihood of a disgruntled employee and what that implies for a system's vulnerability.

SO WHAT SHOULD YOU DO INSTEAD?

Organisations that are serious about preventing IP theft do the following:

- They make the establishment and maintenance of an appropriate risk management regime a core focus of C-level management meetings.
- They take an integrated and cross-enterprise approach to risk assessment.
- They actively work to minimise the chances of narrow box-ticking. Often they'll use the help of third-party risk assessment specialists who can provide an impartial, external view and bring established techniques for capturing all elements of risk.

A narrow and mechanistic approach to risk assessment, however frequently performed, tends to result in important risks being missed

2 ENFORCE HR POLICIES

There's no policy or process guaranteed to prevent the hiring of someone who will later participate in an incident of intellectual property theft. But there's no doubt that an organisation's attitude and approach to hiring is a key factor in minimising the risks of hiring the wrong people, especially for roles that will routinely have access to valuable IP.

The vast majority of the organisations we deal with know in broad terms what HR policies they need, and they tell us that they are serious about enforcing their policies.

In reality, few have sufficiently clear policies at the required level of detail, or the processes to enforce them consistently. And most pay only lip service to the policies they have, inasmuch as it takes little more than a senior manager expressing an urgent need to hire someone quickly, for all sorts of formally required processes to go out the window: references won't be taken up properly, claimed qualifications won't be directly checked with the relevant institutions, and the necessary security clearances will be sidestepped.

There are two things to get right when it comes to HR policies and their enforcement:

- **CULTURE**. If senior managers can bully HR into bypassing policy, or policies generally aren't followed for any other reasons, then everyone — management, existing and new employees, and HR — knows that this is an organisation that doesn't take risk management seriously. You're not just more likely to hire people who aren't what they claim to be, but the willingness to flout policy will find its way into other areas and breed a culture where criminal behaviour is more likely to go unnoticed and unreported.
- **OPERATIONS**. Even if your whole organisation is really committed to taking HR policies seriously, that doesn't necessarily translate into having well-defined policies or robust processes for following through. How clear and easy to follow are your guidelines for taking up references? Where and how do you distinguish between all the different roles in your organisation and what policies and procedures apply to each? How do you keep that up to date? Knowing in broad terms what you should be doing isn't sufficient; you need to be able to translate that into quite specific actionable detail that all the relevant people in your organisation both understand and are empowered to act on.

Establishing a risk-appropriate HR culture and operation requires access to expertise that can bring HR and risk management considerations together in appropriate ways to create the right guidelines and governance. If you don't already have this expertise in house we wouldn't recommend trying to reinvent the wheel. Find a risk management partner that has experience in your industry and has established methodologies and templates to get you going.

3 CREATE A 'NO BLAME' CULTURE

Creating a no-blame culture doesn't mean letting people get away with inappropriate behaviour. It means creating an open and just environment in which staff:

- Know clearly what's expected of them and what the potential consequences of their actions are with regard to intellectual property they may come into contact with.
- Feel able to report suspicious or inappropriate behaviour without attracting retribution — especially if reporting on someone senior to them.
- Know that if they are ever accused of anything, they will be treated with discretion, respect, courtesy and scrupulous fairness.

The importance of detailed role descriptions can't be underestimated. This is far more specific than a job description; it's the formalisation of activities that each role is engaged in so that, for example, a programmer knows exactly who she can and cannot release code to; or an engineer knows precisely how sensitive the designs are that he's working on and how ready competitors are to exploit human weakness to get access to them. People understandably develop informal networks at work and if asked by a colleague to do something that bends the rules, they may do so out of friendship or trust if they haven't been very clearly warned against doing so. The more explicit you can be about responsibilities, consequences and the seriousness with which your organisation takes risk management, the less chance there is of staff circumventing policy and the more chance there is that they'll report it if asked to do so. It won't stop every case of IP theft, but will stop many.

HOW TO FIND THE RIGHT BALANCE

Role descriptions aren't static; they need to be monitored, maintained, updated and continually reinforced through awareness and education initiatives. The aim is to create a state of 'rational alertness', where staff can spot and report potential theft without undue paranoia. Finding the right balance is critical because an overly suspicious culture can cripple business and an overly casual culture won't achieve your objectives of preventing IP theft.

Finding the right balance calls for an iterative learning process: putting in place the relevant policies, processes and controls, implementing educational initiatives, then monitoring the results, discussing them regularly at a senior level and adapting policies, processes, controls and education to move people's attitudes and actions in the right direction.

Again, if you don't have the expertise in house to develop role descriptions, appropriate reporting and investigation procedures, or staff awareness campaigns, find a risk management partner that knows best practices and has advice, templates, tools and services to help you.

The aim is to create a state of 'rational alertness', where staff can spot and report potential theft without undue paranoia

4 PAY ATTENTION TO BUSINESS PROCESS DESIGN

Every business process that comes near intellectual property needs to be looked at carefully, not just in terms of which roles may have access, but how the flow of information may happen. You need to implement appropriate information controls and barriers at all relevant points in these processes and to all relevant roles. These include:

- **DUAL CONTROL POLICIES.** These require two people to authorise specific actions relating to IP or to the systems that hold or process IP. This won't eliminate the possibility of theft since the two authorities may collude, but it makes it much less likely. Having implemented dual controls, it's vital to manage them carefully. We know of companies where internal movement or reorganisation has resulted in dual control residing in a single individual — which rather defeats the purpose.
- **PROCEDURAL CHINESE WALLS.** These prevent information passing between specific functions to minimise the chance of IP leaking to inappropriate places.

THE IMPORTANCE OF IDENTITY AND ACCESS MANAGEMENT

Implementation of these or other information controls requires an appropriate identity and access management regime that gives your organisation very clear visibility and control over who is associated with what roles and permissions at any time, and what they therefore should and shouldn't have access to. Nowadays this mostly comes down to the implementation of appropriate IT solutions, but don't forget that it's just as important to implement appropriate information controls for processes that sit outside of IT systems (for example, manual paper-based processes).

CSC CYBERSECURITY PORTFOLIO

The services that together comprise our comprehensive Cybersecurity portfolio operate both as standalone and as fully integrated capabilities. Of particular relevance to intellectual property protection are:

CYBERCONSULTING. With over 50 years of innovation and experience CSC Cyberconsulting specialises in the creation of both technical and organisational controls designed to provide an appropriate level of mitigation that meets with your stated business requirement and risk profile, enabling users to carrying out their daily business without unreasonable disruption. Talk to us about our Security Consulting services, which cover strategy, governance, security enforcement and regulatory considerations particularly in respect of IPR and Privacy.

STRIKEFORCE SECURITY ASSESSMENTS. 'StrikeForce' is our team of applied security specialists, who include a highly skilled global team of elite ethical hackers and related subject matter experts. They can help you with all of your risk assessment needs, from 'techie' vulnerability and penetration testing to the risks associated with social engineering. Our StrikeForce and Security consulting practices work very closely together to provide you with a credible, empirical and practical view on your risk profile; and then help you move towards your intended future state.

MANAGED SECURITY SERVICES. We offer a range of ongoing managed services to help you maintain and adapt the elements of your IP risk management regime. With three tiers of service — Enhance, Extend and Elevate — there's little we can't monitor and manage for you to help you 'manage by fact' and improve your situational awareness and threat intelligence; talk to us about your requirements.

IDENTITY AND ACCESS MANAGEMENT. We can help you automate your processes for the creation, maintenance, and use of trusted identities and their access to your our Consulting, StrikeForce and Managed Security Services teams.

5 USE TECHNOLOGY WISELY

Technology certainly has a critical role to play in preventing intellectual property theft. What you *can't* expect is for technology to be a silver bullet that will eliminate your vulnerability to IP theft without requiring you to pay attention to the cultural, people and process aspects that we've discussed.

Used appropriately, IT is key to helping you 'manage by fact' because it can tell you what's happening in your systems and network. But effective monitoring calls for a lot of kit that needs to be maintained and adapted as systems and networks change; and it calls for expertise and resource to analyse and make sense of the tons of information gathered. This can be expensive to manage in house. We mentioned earlier that organisations often engage independent consultants to help them assess their risk profile; it's even better if your chosen partner offers managed monitoring, threat intelligence and incident handling services, because the chances are good that they can do it for you both more cost-effectively and thoroughly. It's not only their core business, but they can achieve economies of scale doing it for multiple customers.

IT is obviously also critical in implementing effective cross-enterprise identity and access management as well as all the other controls that your risk management and process design activities call for. For example, there are data loss prevention solutions that can block the use of USB sticks in certain machines or prevent the printing or copying of specific file types — or allow it but raise an alert that tells you who's done it. Or there are identity and access management solutions that can ensure that people leaving your organisation have their ability to download information curtailed at the most appropriate time prior to their departure.

All information security controls should be integrated with your identity and access management system to enable you to control activities based on people's roles and responsibilities.

WHAT NEXT?

We appreciate that it's easier to give advice than to act on it, especially when the advice is predominantly about changing culture, attitudes and behaviour — and about doing multiple different things in a joined-up way. That's where organisations such as CSC can help. We have the experience, knowledge and tools to help you implement the five principles discussed here. We're always ready to engage with you on a no-obligation basis to discuss the risk management issues that matter most to you.

To start a conversation contact: Nick Hopkinson, General Manager, Cybersecurity (Europe), at nhopkinson@csc.com

or Robin Lawrence, Head of UK Cyberconsulting, at rlawrence7@csc.com

WHY CSC?

EXPERIENCE. CSC has over 50 years of cybersecurity experience in some of the most sophisticated and technically challenging organisations across the globe. Our broad capabilities address the entire security lifecycle of an organisation's needs. Our integration approach helps ensure we provide the most efficient, effective and appropriate solution – working in close partnership with our clients – and helping them make best use of their own people and technical capability.

END-TO-END CAPABILITIES. CSC's security consulting practice complements our full range of cybersecurity managed services and solutions. So in addition to helping you assess your risk and recommend mitigating actions, we can help you plan and then implement and manage the changes you need to make. It's this kind of cohesive, integrated approach that is best placed to meet the challenges of protecting intellectual property.

Worldwide CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Asia
20 Anson Road #11-01
Twenty Anson
Singapore 079912
Republic of Singapore
+65.6221.9095

Australia
Level 6/Tower B
26 Talavera Road
Macquarie Park,
NSW 2113
Sydney, Australia
+61(0)2.9034.3000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire
GU11 1PZ
United Kingdom
+44(0)1252.534000

About CSC
The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC leads with an informed point of view while still offering client choice.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."