KeepiNg SecRets

Developing Confidentiality Systems

It's 10 pm in Europe, and you get a call from one of your engineers, working late, frantically preparing a customer proposal to be submitted in US business hours. He wants to put into the submission some extremely interesting material he found on your company's intranet.

Unfortunately, some of this information may have come from a third party. There's no confidentiality notice on this data, but the engineer knows that this third party doesn't always mark its confidential information as confidential. (And you know that the nondisclosure agreement with the third party has a draconian liquidated damages clause for any unauthorized breach of confidential information.)

The engineer also found early test data from some work that one of the project teams is doing. He knows this data is confidential, but he thinks the customer has signed a nondisclosure agreement.

So, can the engineer do what he wants: put all this information in the customer proposal?

By Therese Catanzariti

In order to answer this question—and many others like it—you need to understand the practical issues of protecting confidential information. The law relating to confidential information (UK), trade secrets (US), and undisclosed information (WTO TRIPS Agreement A39.2) varies across countries, and in the US varies across states. However, every jurisdiction requires that the owner of the information has to show that the information is confidential and of some value: One important way to demonstrate this is illustrating what you have done to keep information confidential. And law is only one part of the story—the law is not going to lock your office for you. If you really want to protect your confidential information, you need to take real physical measures to protect the information. If you create or receive confidential information, you should have systems and processes to:

- protect confidential information;
- protect yourself from claims that you are responsible for breaches of confidential information; and
- protect yourself against claims that your business has been contaminated by a third party's confidential information.

The Problem with Nondisclosure Agreements

Confidential information is the lifeblood of any company. Not surprisingly, most companies work vigilantly to prevent the disclosure of confidential information except to those who have signed appropriate nondisclosure agreements (or other agreements containing nondisclosure provisions). These nondisclosure agreements (also known

THERESE CATANZARITI BEc, LLB (Syd), LLM (Lond) is an Australian barrister currently working in Finland as general counsel at Hantro Products, a Finnish company specializing in designing hardware and software video codecs for mobile media devices. She is ACC Europe's country representative for Finland. She can be contacted at *theresecatanzariti@yahoo.com.au.*

as NDAs) impose serious obligations on the recipient to protect the disclosing party's confidential information, and sometimes impose severe penalties for breach of these obligations, such as large liquidated damages.

Unfortunately, many of these agreements are not reviewed as carefully as they need to be. A company's lawyers will typically check that the definition of "confidential information" is broad enough to cover any deliberate or inadvertent disclosure of information by the discloser to the recipient. However, the confidentiality obligations imposed on the recipient are often skimmed over. This is a risky strategy—the obligations are often onerous, such as requiring each employee to sign confidentiality agreements in substantially the same form or to purge all confidential information from the recipient's systems. If a company's lawyers blithely accept these obligations, they may be creating a rod for their own back. It is not enough to review a nondisclosure agreement from the perspective of the discloser. Confidentiality obligations are often mutual, and a discloser may also be a recipient. Therefore, even if a company's lawyers think that the company will mostly be disclosing information, they should also review the confidentiality agreement as if the company were a recipient.

Even the best nondisclosure agreement, however, cannot make the risks of disclosure magically disappear, because the discloser is relying on the recipient's confidentiality systems and processes. A prudent discloser will check precisely how the recipient will be protecting the discloser's confidential information—what sort of systems and processes does the recipient have in place?

And for the same reasons, a prudent company will be checking that its own systems and processes for protecting confidential information are robust.

Your Written Confidentiality Policy

If your company doesn't already have one, we strongly recommend you develop a written confidentiality policy and checklist. There is admittedly a danger that such a policy might, in some future litigation, be seen as a standard of reasonable behavior that your company has failed to reach. However, this risk is outweighed by the advantages of ensuring that your company has something that all its departments and stakeholders can contribute to and then own; something that project managers can use to develop their own checklist; and something your company can provide if asked for by a court, an insurance company, a potential business partner, a potential investor, or a potential acquirer.

Checklist for Employee Security

- Be wary of hiring employees from competitors.
- Put a confidentiality provision in employment contracts.
- Provide confidentiality training for employees.
- Give project members special warnings about project confidential information.
- Keep records which show the projects that each employee has worked on.
- Warn employees about how to behave at conferences and trade shows.
- Remind departing employees of their continuing obligations regarding confidentiality, and ask them to confirm, in writing, they have returned all company property.

Classifying Your Information

You should classify all the information your company possesses into categories of confidential information. The basic categories of information are:

- public,
- confidential,
- company confidential, and
- project confidential.

Public information is all the information that your company can freely disclose. This information can be used, for instance, in marketing materials, press releases, user manuals, company speeches, or your company's internet site.

Confidential information, such as product specifications, is information that your company can disclose if the recipient has signed a nondisclosure agreement or a more comprehensive agreement that includes confidentiality obligations. However, "confidential information" is not all of your company's confidential information—it's just a subset.

Company confidential information is confidential information that your company should not disclose to any outsiders, even if they have signed ironclad nondisclosure agreements. Such information includes early-stage test results, supplier information, pricing information, individual customer terms and conditions, algorithms, and source code. This information is like the capital of your company; it's what the company uses to make money—to make its products and provide its services. Disclosing this type of information is like giving away your factory or machinery. If your company's customers get this information, they may not need your company anymore. If your competitors get this information, they could destroy you.

Project confidential information is information that your company should not use or disclose outside the particular project or a particular team. This includes third-

party information or other confidential information that should only be disclosed to persons who have a need to know. For example, details of the company's shareholder agreement should be restricted to the management team.

These categories can, of course, be modified and additional categories created, in order to suit the needs of your company.

Your company should classify all new information when it is created or received from a third party. For example, the word processing package can prompt the author for a classification when the document is created and then mark the classification on the document.

Classifying information from third parties can be particularly important. Although many nondisclosure agreements (and other agreements with confidentiality provisions) require recipients to protect only information that the discloser marks as confidential, many other agreements contain much broader definitions of "confidential information." It is not unusual, for instance, for an agreement to specify that everything disclosed is protected, or that information is protected if it is reasonable to expect that such information would be confidential. If one of these broader provisions is contained in a nondisclosure agreement, the recipient needs to try and mark all information received from that third party in an appropriate manner, in order to ensure the information is properly handled and protected within the company. If this is going to be practically impossible, you really need to explain this when you are negotiating the NDA and try to narrow the definition of confidential information to information that the discloser marks as confidential.

When your company starts discussions with a third party, your company should appoint one or two persons to coordinate information being received from the third party. These individuals should be responsible for ensuring that the information is properly classified before it is introduced into your company's systems.

Stopping Loose Lips

People are the weakest link in any confidentiality system. The headlines are filled with numerous instances of an audacious industrial spy hacking into a system, or an aggrieved ex-employee downloading vital source code. But it's the inadvertent drip-drip disclosure of customer opportunities, business plans, and product roadmaps that can wear down a business.

The problem occurs every day, when employees are chatting in planes, taxis, elevators, bars, and gyms—and someone just happens to overhear. Each industry has stories about particular flight routes which are excellent sources of information. A friend described one experience as illumi-

---

Checklist for Customers, Suppliers, and Commercial Partners

- Sign an NDA before disclosing any of the company's confidential information.
- Check the NDA Purpose before disclosing information.
- Only disclose confidential information that can be disclosed outside the company, not "company confidential" or "project confidential" information.
- Watermark particularly sensitive information.
- Limit access and use of particularly sensitive information to named individuals.
- Ideally, negotiate liquidated damages for breach of an NDA.

nating as an in-house presentation, complete with Power-Point® slides passed back and forth between colleagues in adjoining rows.

Managing Your Employees

The process of keeping your employees in line should begin even before they are hired. Your company's hiring manager should be wary of hiring people who have worked in a similar position for a competitor, lest that person inadvertently or intentionally use confidential information from that competitor and land your company in hot water. If such a person is hired, they should be counseled against using any information from their previous position, and that discussion should be documented, so as to help insulate your company against liability if the employee disregards his instructions.

When a new employee is hired, his or her contract should include confidentiality provisions requiring that employee to keep all of the company's sensitive information confidential. This particular part of the contract should be explained to the new employee by the hiring manager to ensure that the employee fully understands what is expected of him or her.

As part of a new employee's training, the induction program should include a module about confidentiality. The employee should thereafter receive regular training on this subject (say, once a year). This continuing training can take the form of large lectures or individualized online training modules. There should be a written record that the employee has completed training (e.g., an attendance sheet).

If there is a project involving project-specific confidential information, the project's kick-off meeting should include a reminder that the project-specific information must be used only within the project and cannot be used on other company projects or discussed with other compa-

ny employees who are not project members, or discussed in open company areas like the staff canteen or coffee room. This reminder should be recorded in the meeting minutes.

Your company should keep records on all employees that list the various projects each employee has worked on. This can help your company avoid problems caused by assigning an employee to work on an inappropriate project. For instance, if an employee has worked on a project involving third-party information which is similar to information being developed by your company in a new project, that employee should not be selected to work on the new project. (If the employee has to be assigned to the new project, the employee should of course be counseled against using the third-party information, and this warning should be documented.)

Before your company's employees attend trade shows or conferences, they should be reminded at a pre-meeting not to discuss company business or make cell calls about company business in open spaces such as on the plane, train, bus, or taxi to and from the event, during a coffee break, on the trade floor, or at surrounding cafes or restaurants. And when they catch up with old professional friends and colleagues at the conference, they need to avoid discussing their current or recent work.

Whenever an employee leaves your company, the employee should be reminded in the exit interview of their continuing confidentiality obligations. The employee should also sign to confirm they have returned all copies of the company's confidential information.

Keeping Tabs on Subcontractors and Independent Consultants

If your company wants to disclose confidential information to a subcontractor, you need to ensure that the subcontractor has effective systems and processes in place to protect this information. Start before a subcontractor has been selected for a project. Your company should ask each potential subcontractor to explain how they protect confidential information. This should be one of the factors used to select a subcontractor for a particular job.

The subcontracting agreement should require the subcontractor to use the same level of care it uses to protect its own confidential information (but no less than reasonable care) to keep all of the company's confidential information confidential. It should also require the subcontractor to impose similar confidentiality obligations on all its employees.

The agreement should specify what serious consequences will occur if the subcontractor or any of its employees breaches the confidentiality obligations. The agreement could state, for instance, that a breach would allow your client to immediately terminate the project and/or collect a significant amount of liquidated damages.

Checklist for Subcontractors and Independent Consultants

- Select subcontractors/consultants who have good systems for protecting confidential information.
- Put confidentiality provisions in contracts with subcontractors/consultants.
- When subcontractors/consultants work on your premises, remind them in writing of their confidentiality obligations.
- Be wary of sharing third-party confidential information with subcontractors/consultants.

It is also important for the subcontracting agreement to provide your company (or a representative) with the right to audit the subcontractor's premises, systems, and processes, in order to ensure that confidential information is being properly protected.

When employees of a subcontractor arrive to visit or temporarily work on any of your company's premises, they should report to reception and sign a confirmation that they will not use or disclose your company's confidential information. The receptionist should briefly explain what this confirmation is. The confirmation should be written in English and the language of the country where the office is located.

Before your company shares any third-party confidential information with subcontractors, you should check your company's nondisclosure agreement with the third party. Such agreements sometimes prohibit disclosure to subcontractors, allowing the information to be seen by only the employees of the contracting party (that is, your company's employees only, and not your subcontractor's employees).

Your New Best Friends

A company has to disclose information to customers, suppliers, and other commercial partners in order to stay in business. However, there is a risk that a company might disclose too much confidential information or disclose confidential information without proper protection. It is tempting—the NDA may take time to negotiate and the customer may disappear. But the short-term advantage of the quick

sale may do long-term damage to the company's assets.

The company should not disclose any confidential information to another company without both signing a nondisclosure agreement. The nondisclosure agreement should require, at a minimum, that a party only use the other's information for the purposes of the business relationship between the parties, and will use no less than reasonable care to protect the confidential information.

The company should always check the nondisclosure agreement before it discloses any confidential information. It should make sure that the nondisclosure agreement is still valid and has not expired. And it should check that the purpose in the nondisclosure agreement is relevant to the purpose of the current business case—the company may have signed a nondisclosure agreement with a view to a particular business case and may have limited the purpose to the particular business case. The purpose in the nondisclosure agreement may be completely irrelevant to what the company is now planning to do.

The company should not disclose all of the company's confidential information to its customers, suppliers, or commercial partners, even if they have signed a nondisclosure agreement. The company should only disclose a subset of its confidential information, and should only disclose information which is not "company confidential" or "project confidential."

If a company is disclosing particularly sensitive information, it should try and mark the information so it is recognizable as the company's information. For example, software code can include watermarks embedded into the code so that the program will react in a certain way to certain commands.

If a company is disclosing particularly sensitive information, it should also try and track the information through the recipient company. For example, it can require the recipient company to limit access and use of the information to the individuals listed in the nondisclosure agreement.

A company may also include liquidated damages for breach of the nondisclosure agreement. The risk of liquidated damages provides a strong incentive for the recipient to improve their confidentiality systems and processes. You should note, however, that liquidated damages are difficult to negotiate.

Physical Security

In order to properly safeguard confidential information, physical security is essential. Your company's office premises should be locked and access restricted by key, identity card, or password/passcode. If a password/passcode is used, it should be regularly changed. This assures that it will become useless within a relatively short period so that

Checklist for Physical Security

- Lock premises and restrict access via key, identity card, or password/passcode.
- Limit company information on ID cards.
- Lock windows that are easily accessible from the outside.
- Put fax machines and copiers in appropriate areas.
- Teach employees to shred all unnecessary copies of confidential information.
- Restrict access to filing cabinets.
- Clean whiteboards after each use.
- Restrict access to computers via passwords or other ID verification.
- Set Unattended computers to automatically lock and to black their screens.
- Require ID verification to use any mobile communications device, such as a Blackberry®.
- Before scrapping or reusing equipment, erase hard drives, disks, and so forth.

it cannot be used by ex-employees or someone outside who has found it out. It's amazing how often this is overlooked. For example, during Air Canada's recent litigation with WestJet, Westjet admitted some of its employees had accessed Air Canada's password-protected employee website to access Air Canada's confidential flight schedule information by using a still-active password of a former Air Canada employee.

If a project involves project-specific confidential information, such information should be kept in a separate section of the premises with access restricted to project members.

If your client uses identity cards, each card should include the person's name, ideally accompanied by a photograph. It should also identify any access privileges to particular restricted areas. The identity card should not, however, list your company's name or any other identifying features of your company, including its office address. This assures that if the card is left on a bus or at an airport lounge, the person who finds it has no idea where it can be used. Ground level and other accessible windows should be locked.

The fax machine and photocopier should be kept within your company's premises, not in a shared office area. This makes sure that the company can quickly protect any confidential information it receives, rather than the information sitting for a few hours in an in-tray, available to everyone else who uses the shared office.

If a project involves project-specific confidential information, there should be a dedicated fax machine and photocopier within the project area. If this is not possible, project members must be advised to promptly collect all copies of project-confidential information.

Your company should shred all unnecessary copies of confidential information, subject to your company's document retention policy. A project that involves project-specific confidential information should have a dedicated shredder.

Shredders don't do any good unless they are used, and surprisingly, it often takes new employees several months to locate the company's shredders. To avoid this problem, at the time of their induction, all your company's new employees should be advised where the shredders are.

Filing cabinets should be locked, with restricted access. If a project involves project-specific confidential information, the filing cabinet should only be accessible to project members.

All whiteboards should be cleaned at the end of each meeting, and as a precaution, at the end of each day. If possible, each project should have its own project-specific meeting room, or its own portable project-specific whiteboard.

ACC and Other Extras on . . . Protecting Confidential Information

ACC Committees:
More information about these committees is available on ACC Online℠ at *www.acca.com/networks/committee.php,* or you can contact Staff Attorney and Committees Manager Jacqueline Windley at 202.293.4103, ext. 314, or *windley@ acca.com*.
• Corporate & Securities Law Committee
• Information Technology Law & eCommerce

***Docket* Articles:**
Eileen Barish, Brent Caslin, "Before Signing Your Next Nondisclosure Agreement, Count to Ten," *ACC Docket* 24, no. 1 (January 2006) 24–34. *www.acca.com/resource/v6643*.

Sample Forms and Policies:
Other forms and policies are available by searching ACC's *Virtual Library℠* at *www.acca.com/resources/vl.*
• Confidentiality Information Provisions (2005). *www.acca. com/protected/forms/confidential/provisions.pdf*.

• Mutual Confidentiality Agreement with Nonsolicitation Clause (2005). *www.acca.com/protected/forms/agree/ mutual_confidential.pdf*.
• Nondisclosure Agreement Guide (2005). *www.acca.com/ resource/v6273*.
• Nondisclosure Agreements Checklist (2005). *www.acca. com/protected/reference/nondisclosure/lastminute.pdf*.
• Product Development Confidentiality Agreement (2005). *www.acca.com/protected/forms/intelprop/productagree.pdf*.
• "Responsible Information Handling," a quick reference (2005). *www.acca.com/protected/reference/privacy/info-handle.pdf*.

InfoPAKs:
• Intellectual Property (2005), *www.acca.com/resource/v5791*.

Leading Practice Profile:
• Privacy and Data Protection: What Companies Are Doing (2006). *www.acca.com/resource/v6679*.

All your company's desktop computers and laptops should have passwords or other systems for identifying authorized users (e.g., fingerprint ID). If passwords are used, the system should prompt employees to regularly change their passwords.

If a computer is unattended for a specified period, its screen should go black and the machine should automatically lock. Laptops used by mobile staff should ideally be fitted with screens which stop people sitting near the users from viewing the screens.

All mobile phones, PDAs, and Blackberrys® used by company employees should have passwords or other systems for identifying authorized users. Passwords should be regularly changed. How many of your company's mobile phones still have the factory-set password 0000 or 1234?

Before a computer or other hardware device is scrapped, its hard drive should be thoroughly erased. Similarly, all tapes and discs should be erased before being recycled or physically destroyed.

Remember, however, that physical security is only as strong as the individuals using it. Many people who have worked in companies with partitioned areas know only too well that if you forget your pass, the easiest way to get in is to knock on the glass door, smile sweetly, and ask someone to let you in.

Network Security

Your company's network should have firewall and virus protection software, of course. Moreover, in order to log in to the network, users should be required to input a password. This log-in requirement should cover connections from desktop computers, laptops, PDAs, Blackberrys®, and mobile phones. Remote users should enter the network only via a secure network connection. For example, the network connection should only be activated if there is a password entered.

Sensitive electronic documents should be locked and access restricted through methods such as passwords or encryption. If certain documents are likely to contain confidential information, the templates for these documents should be preformatted with a header or footer that has "confidential information" in boldface.

Your company's intranet should be available only to employees, and it should be accessible only via the network. It may be desirable to allow subcontractors to access certain sections of this site, but they should not have unrestricted access to the whole intranet site. Similarly, if a project involves project-specific confidential information, there should be project-specific intranet pages which are restricted to project members.

Your company should have encryption technology, which it can use to receive and disclose sensitive information online.

Your company's email policy ought to include a section on disclosing confidential information. The email system should be set up so that a confidentiality statement automatically appears at the bottom of each email being sent. This confidentiality statement should make clear that all information in the email is confidential unless marked public. However, the confidentiality statement is not a magic shield—we have all received (and passed on) jokes and gossip in an email with a confidentiality statement on it. Even if there is a confidentiality statement on all outgoing emails, employees should be warned not to send any information by unencrypted email that they would not be comfortable reading on the front page of the newspaper or the *Drudge Report*, because that's where leaked emails sometimes end up.

All sensitive information should be encrypted. Employees should also be reminded not to send company information through public email accounts such as Yahoo®, Hotmail®, or Gmail™ unless they have effective encryption. Your company's email system should be configured so that all incoming emails that originate outside your company are not simply filed in the recipient's inbox. Instead, the email should be placed in a separate mail folder organized by project or other name. If this is not technically reasonable, employees should be advised to file incoming external emails into mail folders as soon as reasonably practicable. This helps the user to quickly identify emails from third parties so that these messages can be returned or destroyed, if required by the third parties. For example, many nondisclosure agreements require the recipient to return or destroy all confidential information at the end of the business cooperation between the companies. Some even require that an authorized officer certify this. It's very difficult to do if the emails containing confidential information are all over the place.

Checklist for Network Security

- Ensure network has up-to-date firewall and antivirus software.
- Require password to log into network.
- Restrict access to sensitive electronic documents.
- Limit access to the company's intranet.
- Use encryption technology to receive and disclose sensitive information online.
- Be sure appropriate email policy is in place.
- File emails arriving from outside the company into special folders.
- Place a confidentiality statement automatically at the bottom of each email.
- Use special email addresses for individuals handling project-specific confidential information.

If a project involves project-specific confidential information, the email addresses of the project members should be configured so that their email addresses include the project name. Thus, before sending any project-related email, a sender can easily check that the addressees are all, in fact, project members.

You Can't Always Hide Your Mistakes

One of the most powerful word processing tools in contract negotiations is revision mode. No more unreadable handwriting on a smudged fax—you can clearly mark up the changes you want and then accept the proposed changes that you are willing to accept. But how much information are you giving away? Many revision mode programs will reveal the name of the reviewer and the day and time the revision was done. This may be very useful to your negotiating counterpart—they can identify whether it was a legal person's change or a business person's change—and more directly target their response.

But doesn't all this go away when you accept changes? Alas, no. Many counsel use revision mode internally to collate all the comments and changes of all the different stakeholders. When everyone is happy, counsel accepts all the changes to create the final document ready to be sent out. However, hidden away in an "accept all changes" clean document may be the marks of the previous changes. More worrying than revealing just the reviewer's name and time of the review, hidden away in the clean document may be all of the actual changes that were proposed and then rejected internally, before the apparently clean document was sent out. This includes changes proposed by the business person but further changed or rejected by legal, or changes proposed by legal and rejected by business. This may disclose the negotiating strategy, or may disclose rifts within the negotiation team: a bounty of information for your negotiation opposing counsel.

To avoid this potential disaster, one strategy is to accept all changes in the document and then save it as a new document. Alternatively, you can abandon Word® and turn the document into an Adobe™ Portable Document Format (PDF).

Audits

Your company should have regular audits to assess the strength of its confidentiality systems and processes. These regular audits should involve and be actively supported by senior management—this is about core assets. The audit may be a specific audit or part of a more general audit—for example, the project manager could include confidentiality modules as part of the project audit and the project wrap-up. The confidentiality processes and checklists can be used as the basis of the questions that need to be asked as part of the audit. For example, all software used by the company should be checked for vulnerabilities to attacks, viruses, and espionage. You should use information from the audit to highlight risk areas that need to be more actively monitored,

ACC International Resources on . . . Confidentiality

For more on how the international legal community addresses this topic, see the following resources:

- Jeffrey D. Adelman, Paula Barrett, and Brent V. Bidjou, "Pitfalls and Landmines in Privacy and the Collection, Use, and Security of Personal Information 110," ACC 2005 Annual Meeting course material. *www.acca.com/am/05/material.php.*
- James R. Beyer and E. Johan Lubbe, "Clash of the Titans: Complying with US Whistleblowing Requirements While Respecting EU Privacy Rights," *ACC Docket* 24, no. 4 (April 2006): 22–36. *www.acca.com/resource/v7105.*
- Klara Burianova and Alice Turinas, "Avoiding the Latest EU Data Protection Pitfalls: Changes in European Privacy Laws That Restrict Emarketing," *ACCA Docket* 21, no. 6 (June 2003): 92–101. *www.acca.com/protected/pubs/docket/jj03/eudata1.php.*
- Confidentiality Agreement (Romania), *www.acca.com/protected/forms/employment/confidential.pdf.*
- Confidentiality Agreement (sale of shares, UK), *www.acca.com/resource/v7403.*
- InfoPAK: Data Protection—A Practical Guide to Personal Data Transfer Laws in Europe, Canada and the U.S. (2005), *www.acca.com/infopaks/data_protection.html.*
- Webcast: "Whistleblower" Anonymous Hotlines and SOX—Dealing with the French and German Decisions (November 17, 2005), *www.acca.com/networks/webcast/.*

Checklist for Using Revision Mode

- Using revision mode in word processing can inadvertently reveal sensitive internal negotiation strategy.
- If you have used revision mode in your Word® documents to collate internal comments and changes, you should accept changes and then save the document as a completely new document.
- Alternatively, you should save the document as an Adobe™ PDF.

and where training needs to be improved. You should also conduct regular audits of your subcontractors' confidentiality systems.

Knowledge Is Power

A company's assets are just a random jumble unless you know how they all fit together and know how to work them to run the business. Confidential information and trade secrets are key—know-how, production processes, marketing lists, industry understanding, business plans, and product roadmaps. As the world economy moves from factories to information, knowledge is the key competitive advantage.

But confidential information and trade secrets are fragile assets—they are only valuable if they are actively protected. A company needs to introduce systems and processes to protect its own confidential information and trade secrets. And if a company wants to access another company's confidential information, it needs to show that it can protect the other company's confidential information and trade secrets. Make sure your engineer knows why he needs to respect the third party's confidentiality and can't include the third party's confidential information. And that he or she knows why they can't give away the company's strategic assets by disclosing early stage project results. Which means he or she can spend more time finding the information that *can* be used and can prepare a great customer presentation instead of trying to answer difficult legal questions. And, you can get some sleep! 🄰

Have a comment on this article? Email editorinchief@acca.com.

For Additional Information

- J. Armstrong, M. Rhys-Jones, and D. Dresner, "Managing Risk: Technology and Communications," LexisNexis UK, 2004
- F. Gurry, "Breach of Confidence," Oxford University Press, 1984
- "What An Employee Needs to Know," WIPO Fact Sheet, *www.wipo.int/sme/en/documents/employees_ confidentiality.htm*
- WTO Summary, *www.wto.org/english/tratop_e/trips_ e/intel2_e.htm#tradesecrets*