

Viewpoint Paper

**Confidentiality & the Certified Confidentiality Officer:  
Security Disciplines to Safeguard Sensitive/Critical Business Information**

John Kanalis CCO, CPO, CSSMP, CPOI  
Business Espionage Controls & Countermeasures Association (BECCA)  
BECCA Europe Administrator

**Introduction**

Confidentiality is the ethical and professional duty not to disclose inappropriate information to a third party. Confidentiality may apply because of the legal or ethical requirements of certain professionals, such as those who hold Certified Confidentiality Officer (CCO) certification (See <http://www.becca-online.org/ccoprogram.html>) In business, confidentiality exists to protect the privacy of a business entity, including its critical or sensitive business information. Policies and procedures are needed to safeguard against espionage and/or intentional or unintentional disclosure of sensitive or proprietary information. These policies and procedures may be mandated by laws or regulations, or by the professional ethical obligations of employees. These policies and procedures may also be implemented as a best practice to help decrease insider or outsider access to critical business information.

The lack of preplanning regarding the flow of confidential information within the business environment can result in misunderstandings about safeguarding critical business secrets and preventing thefts of intellectual property, including property protected by copyrights, trademarks, and patents. (See [www.BECCA-online.org](http://www.BECCA-online.org))

A confidentiality vulnerability audit is an initial step to business's minimum requirements of being protected against danger or loss. (See John Kanalis, 2008, BECCA Training in Business Espionage Controls & Countermeasures). This is a fact-finding, non-fault-finding audit that involves:

- a search for vulnerabilities through information collection and analysis, and
- a way to identify leaks, sources, & indicators potentially exploitable by an adversary;

There are a number of reasons why business confidentiality can be important. These include:

- Trade secrets and intellectual property often need to be kept from business competitors.
- The improper dissemination of information about current business objectives or future projects may harm the business.
- Confidentiality may be necessary for employee security, and for the security of their families.
- Job security can be an issue.
- Confidentiality provisions may help to encourage employees to make use of services designed to help them, such as counselling or other employee assistance programs.

-Assurance of confidentiality may make it easier people to seek help without fear or damage to reputation or other relationships.

Confidentiality is based on four basic principles:

1. Respect for a business's right to privacy.
2. Respect for human relationships in which business information is shared.
3. Appreciation of the importance of confidentiality to both the business and its employees.
4. Expectations that those who pledge to safeguard confidential information will actually do so.

Confidentiality is necessary for the best interests of the organization, or because disclosure of the information will cause significant damage to the business itself or to other organizations. The need for confidentiality exists when information is designated as "confidential" (e.g. stamped or announced). It also applies where the need for confidentiality is obvious or evident (depending on the nature of the material or context of the situation), or when required by applicable law—even when the information is not specifically designated as confidential.

Typically, it is not solely up to the individual to determine what is and is not confidential. If the organization considers and treats information as confidential, then officials and employees of the organization must respect that need for confidentiality. Moreover, individuals must not be permitted to arbitrarily overrule or disregard their duty to maintain confidentiality.

Business officials and employees are often legally required to keep certain business and personal information confidential. This legal obligation exists even if officials and employees have not signed contracts or other documents related specifically to confidentiality.

Board members in particular have been placed in a position of trust, and it is their fiduciary responsibility to honour the business's need to keep certain information confidential. A Board member or employee who discloses confidential information can create significant legal liability for the organization if he/she is legally required to maintain confidentiality. The Board member or employee may also face personal liability as a result of disclosing confidential information.

## **Postulates**

I propose here 10 postulates about confidentiality in the business world.

1. The first postulate is that a dynamic security mechanism is needed to prevent losses (loss = cost) that will facilitate the accomplishment of objectives, namely the continued smooth operation of the business while ensuring:

- The security of business structure (both tangible & intangible elements);
- The security of employees and materials;
- The security of information, communications, & information systems that are used to manage risk (risk = intention + ability + opportunity), whether the risk is personal, human, physical, technological, or otherwise has an impact on the organization's well being.

The second postulate is that this security mechanism must, if it is to be effective in managing the foregoing risks and impacts, involve:

- Prevention;

- Tracking;
- Corrective actions.

The third postulate is that the security mechanism needs to be exposed to real-time, tactical assessments that take into account:

- The risk or threat to the whole business;
- The acceptable level of risk or threat;
- The processes of reacting to a threat;
- The need to reduce the overall vulnerability.

The fourth postulate is that this security mechanism, if it is to be effective and produce tangible results, must specifically address:

- Policies for how to implement the security mechanism;
- Procedures detailing the implementation process.

The fifth postulate is that all of the above issues must be integrated into a coherent program, which I call the “Security Program” or “Security Master Plan”.

The sixth postulate is that current business risks are linked to each other, creating a complex co-dependency. Thus, the management of initial frontline responses (e.g., guard actions and responsibilities at a building entrance) has passed into the arena of comprehensive security management.

The seventh postulate is that security strategy must determine the procedures for understanding the nature of risk in detail, in addition to specifying the response plan.

The eighth postulate is that the security mechanism must collect and disseminate information about security-related business processes and how the security mechanism may affect profitability, the flow of information, and the reputation of the business.

The ninth postulate is that the security mechanism, if it is to be effective, must analyze recruiting information from different sources (and in collaboration with others), and use this information to help protect the business.

The tenth postulate is that the security mechanism must have planned—in advance—what happens on the next business day after a serious adverse event. The vast majority of organizations and institutions do not anticipate crises or manage them effectively once they have occurred. Neither the mechanics nor the basic skills are in place for effective crisis management (Managing Crises before They Happen – Mitroff, 2001).

## **Crises and Continuity**

The Institute for Crisis Management ([www.crisiexperts.com](http://www.crisiexperts.com)) defines a business crisis as a problem that:

- 1) Disrupts the way an organization conducts business, and

2) Attracts significant news media coverage and/or public scrutiny. Typically, these crises are dynamic situations that threaten the economics and well-being of the organization and its employees.

Most business crisis situations, such as loss of critical/sensitive business information, may be either sudden or chronic, depending on the amount of advance notice and the chain of events in the crisis. The risk to sensitive and/or critical business information continues to increase significantly as adversaries—both domestic and foreign—focus their espionage resources in even greater numbers on the private sector.

Business continuity can be aided by the use of Sensitive Information Risk Analysis (SIRA) and Evaluation of Sensitive Information (ESA) to reduce and manage the risk of espionage. The development and implementation of rules, policies, procedures, audits, and continuing assessments for the purpose of avoiding the competitive loss of business secrets is an important part of the overall security framework.

Confidentiality applied as a stand-alone process can help identify whether complete pathways exist that link to a potential “window of opportunity”.\* Conservative assumptions can also be useful to estimate business exposure based on indicators & facts.\*\* Another important element is gaining strong support and commitment to the process from the organization’s executive management.

## **Conclusion**

Confidentiality is a prerequisite in any internal or external business transaction. A Certified Confidentiality Officer (CCO) is a security professional who can be of help. He or she has specific knowledge of how to avoid loss, protect critical/sensitive business information, safeguard proprietary information, and enrich a business’s awareness and training on confidentiality issues. Moreover, a CCO can integrate into organization’s philosophy and culture the idea that the “Nothingness Treaty” (nothing happened yesterday, nothing happened today, nothing will happen tomorrow) is a poor philosophy for protecting an organization and its employees.

---

\* See, for example, Roger G. Johnston, “How to conduct an Adversarial Vulnerability Assessment”, Vulnerability Assessment Team, Los Alamos National Laboratory, 2006.

\*\* See, for example, E.G. Bitzer and R.G. Johnston, “Creative Adversarial Vulnerability Assessments”, Vulnerability Assessment Team, Los Alamos National Laboratory, 2006.