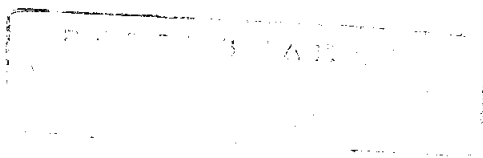# THE ACTIVE LOSS PREVENTION INITIATIVE

VERSION 2.0
JUNE 2002

Robertas Ivanauskas
Arvydas Pajuodis

Faculty of Economics of Vilnius University Faculty of Economics of Vilnius University, Sauletekio ave. 9, LT-2040.

1

Table of Contents

Table of Figures

1 Summary

1.1 In Brief

The Open Group's Active Loss Prevention initiative is a new, strategic enterprise-wide approach to creating the trust, security, and reliability necessary for eBusiness to realize its full potential. Instead of the present, piecemeal, technology-driven approach to eBusiness and security, Active Loss Prevention brings together commercial, professional (legal, audit and insurance), and technology disciplines to create and drive the adoption of verifiable standards of eBusiness best practice.

1.2 Executive overview

Despite the challenges or risks, business leaders around the world are demanding the rapid deployment of eBusiness so that their companies may enjoy the real business benefits offered by this new technology and business process change. They see their current competitors pushing ahead with eBusiness and new competitors with lower-cost models challenging them. They dare not be left behind. The cost savings to be derived from eBusiness are irresistible and the improvements in efficiency, delivery, and customer relationships are undeniable. Senior managers will deploy eBusiness, and concerns about the risks (or indeed any other ancillary issues) will be overruled.

It has become increasingly difficult to identify boundaries of responsibility, especially due to the complexity of systems and the range of risks. Not all are technical, though many IT security vendors will argue, "they have *the* technical solution for all your needs." The approach to understanding the threats and vulnerabilities now needs to become multi-disciplinary due to the interconnectedness of all enterprises.

Many strategic and operational decisions are made using information generated by, or completely dependent upon, highly complex, interconnected, and devolved IT systems. Company officers seek assurance that there are sufficient controls in place to ensure the availability and integrity of this computer-dependent information, as well as being assured that the liabilities of all parties are understood. Businesses require adequate insurance cover for the risks associated with eBusiness. Insurance policies in this emerging area are immature and address only the most obvious dangers. Governments, regulators, industry forums, businesses, and customers will all require that eBusiness processes and technology be adequately and accurately audited for propriety, resilience, and accuracy.

Many commercial organizations are part of, or linked to, the national critical infrastructure. Many transnational organizations operate national water supply systems and gas and oil storage and delivery and electrical delivery. Transportation, banking and finance and telecommunications (including the Internet), are often not seen as part of the critical infrastructure, but in today's interconnected world, they now have a considerable part to play. In addition to that are the emergency services and Government operations. The work of the Active Loss Prevention initiative will fully support the work of critical infrastructure organizations around the world. It is expected that some projects could result in joint work programs.

The Active Loss Prevention initiative is a new approach to addressing all the above issues through the proactive management of information and eBusiness risks for business advantage. It differs from existing approaches in four key dimensions:

- It is a strategic, international, enterprise-wide approach involving commercial, professional (finance, audit, insurance, legal, and technology), human and technical issues.

- It is proactive, anticipating risks, their impact, and spread. Then enabling the tools required to manage the risks.

- It delivers the way forward such that products and processes backed by global standards can be tested, proven, certified, and backed by codes of practice and (where necessary) legislation.

2 Introduction

This new initiative of the members of The Open Group, Active Loss Prevention, results from the concerns of many its active members with respect to both companies and critical infrastructures. This paper is intended to stimulate discussion and document the status of views/concerns/ideas in order to provide a common source for action. It is a living document (this is the second issue) to provide a common basis for communication and description of the scope of work.

2.1 Background

In late 2000, The Open Group identified, through its members' input and speakers comments at subject specific conferences, the need to create an environment where trust and confidence are easily established, and an understanding of the government and business views of the legal and liability issues of securing eBusiness. Several important questions emerged, in four main areas:

- How to apply the laws of liability in an eBusiness transaction

- How to insure an eBusiness transaction

- How to communicate risk or trust information between trading partners

- How to relate technical risk and business risk

Subsequently, The Open Group commissioned a study and discovered that while there are many niche-focused subjects that are being addressed, there is no group that is taking the holistic approach to address these issues and that an initiative was needed. This has been confirmed at the inaugural Active Loss Prevention meeting in Amsterdam during October 2001, leading to the instigation of a range of activities, that includes workshops and the initiation of a number of projects.

2.2 Audience

This paper is intended for business, financial, legal, insurance, and audit professionals involved with the IT-enabled eBusiness world. It is also to assist the Information Systems security community to better understand the needs of the business community.

3 The Story So Far: The Legacy View of IT Security

For a long time, security has been seen as an afterthought; often it is described as being obstructive and unnecessarily expensive. This has led to managers and company executives "taking the risk" and often being ignorant of the risks. In the era of IT systems being constrained to the organization, and often being proprietary to the organization, the risks were seen as mainly due to internal activities. Due to the perceived need to measure the return on investment (ROI) for IT security procurement, business cases stalled; since identifying the likelihood of risks occurring was difficult, no ROI could be identified. This scenario has changed greatly with the advent of the Internet where enterprise systems are being seamlessly integrated together. At a minimum, external access to enterprise Web servers has opened up the enterprise boundary to outsiders.

Criminal activity will happen. The business protocols in use have grown over many years to combat fraud, embezzlement, and theft. It is the mistaken belief that using computers doesn't change the picture that has caused many to ignore the additional or different threats that result.

Loss of data or system availability can happen, even when the organization is prepared and knowledgeable, through disaster, software bugs, and administration errors. When not prepared or knowledgeable, then there is *also* an exposure to malicious and criminal activity resulting in intellectual property loss or destruction and proprietary data exposure as well as network access being disabled. The result can be massive national shutdowns of servers and can be as costly as power or water shutdowns – i.e., a failure of the National critical infrastructure.

There are four main reasons why information security is failing today:

- It focuses on only a small part of the problem of information risk. The security concerns applied by security technologists are applied to a single piece of technology, whereas the system is composed of many aspects – many diverse, but integrated technology pieces, and business and social elements. The security technologist, often working on one component of the system, may be aware of the generic threats to such a component, but is often unaware of the broader environment into which that component is placed. Additionally, systems are becoming increasingly complex and inter-dependent across organizational boundaries.

- It does not do a satisfactory job of protecting businesses against even that small part. The annual FBI/CSI computer crime surveys and the CERT Coordination Center annual summaries have shown substantial increases in the number of security incidents and dollar losses resulting from such incidents in each of the past five years. But at the same time, the Year 2000 FBI/CSI survey also reports that use of information security technologies is very widespread – close to 100% of companies that responded to the FBI/CSI survey use anti-virus, firewall, and access control technologies. This combination of nearly universal deployment of security technology with rapidly and steadily rising losses strongly suggests that security is not being properly managed – countermeasures are installed and then forgotten.

- Enterprises rarely rigorously use the solutions already available to them. They lack consistent policies, procedures, sanctions, and education to ensure the integrity of information and eBusiness systems that they demand in other critical areas such as finance, health and safety, and product liability.

- Security is expensive[1], not only in financial terms, but especially in the perception of interference with daily work (in that it often disables "short cuts" in procedures). It has no value when there is no attack (or natural/accidental disruption in the system environment). Consequently, people tend to use as little of it as they think they can get away with. Moreover, there are no widely accepted metrics for characterizing security, so it is difficult

---

[1] Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, National Academy Press, Washington, D.C., 2002

for a decision maker to know how much security a certain investment buys or whether that investment is enough

The result is that security risks are increasing. Many simply deny the problem or ignore it. As a result (or probably because of it) there is a lack of proper threat assessment foe assets and the development of protective measures for them. There is an acceleration of new technologies with no security capabilities (not asked for or offered) and often an improperly designed infrastructure of existing systems, applications, networks, etc. There is no obvious legislative requirement to address information security specifically (though through an understanding of company law one can interpret a need) and senior management does not properly recognize the risks.

4   The Future of Business and the Need for Change

For the purpose of this paper, the term eBusiness includes all forms of commerce conducted via the exchange of information across electronic networks, at any stage in the supply chain, whether within an organization, between businesses, between businesses and consumers, or between the government and private sectors, whether paid or unpaid.

EBusiness is important because of its dramatic growth and potential, its ability to demolish existing market barriers (geographic, cultural (custom and practice), market separation, and business scale). The way it enables increased efficiency within existing business models, and the way it transforms existing business models makes it an obvious area for investment.

Technology is becoming more robust and affordable. Businesses can easily put their processes on line and connect to their employees, trading partners, customers, and suppliers. Employees are being retrained, processes are being redesigned, and new technical solutions are being integrated. It is these changes that are providing benefits to corporations large and small. This enabling technology has allowed companies to manage their businesses differently, to inform their employees better, and to create the best trading environment for the company, its customers and suppliers. It has enabled companies to react faster to market desires and changes and to support the constant creation/dissolution of partnerships and alliances between businesses. Companies may now cooperate in one context but compete in another. Within this complex business environment, they need new tools and processes to manage the risks created by the connected approach to business.

Despite the challenges or risks, business leaders around the world are demanding the rapid deployment of eBusiness so that their companies may enjoy the real business benefits offered by this new technology and business process change. They see their current competitors pushing ahead with eBusiness and new competitors with lower-cost models. They dare not be left behind. They see new competitors entering their market spaces, free from legacy processes and other baggage, and deploying the new technology from scratch. The cost savings to be derived from eBusiness are irresistible and the improvements in efficiency, delivery, and customer relationships are undeniable. Senior managers will deploy eBusiness solutions and concerns about the risks (or indeed any other ancillary issues) will be overruled or ignored because they take calculated risks or, more likely, do not calculate risk at all.

Businesses and consumers are concerned about fulfillment of orders. Businesses are concerned about the enforcement of contracts. Internet Service Providers (ISPs) are becoming concerned about liability for customers' content on their systems. The whole area of eBusiness law is immature and incomplete – everyone views it as a major weakness to the robustness and attractiveness of eBusiness. An extra dimension is added when we consider the potential for cross-border disputes. The legal community has started to address some of the issues raised by eBusiness; however, knowledge and skills are in short supply.

There needs to be a clear means of resolving disputes about eBusiness transactions. For credit card transactions, there is a proven route and processes for redress. But this comes at a price. Internet transactions represent 2% of business but 50% of card disputes (Visa survey 1999). Most disputes are over charges for unordered goods, late delivery, and additional charges. Given this scenario for relatively simple transactions, the more complex and larger value of B2B transactions opens up many more liability issues. Simple questions, such as who takes liability, when does it transfer from one party to another, etc. are not, yet, answered.

Businesses require adequate insurance cover for the risks associated with eBusiness. Insurance policies in this emerging area are immature and address only the most obvious dangers. Furthermore, the knowledge of insurance companies is limited about loss prevention in its widest sense, and in many cases they are unable and unprepared to advise and assist their clients on ways to reduce exposure.

However, there are issues here in both the Underwriting and Client areas. Underwriters and Brokers have a lack of understanding regarding cyber and risk management issues and, indeed ask the question - "will traditional insurance provide cover?" Several legal cases seem to be pointing this way. There is a lack of accurate loss information. Some organizations do not wish to declare it (and may self-insure) and there is not a common vocabulary to record losses in a consistent way for those who do declare losses. From a client perspective, they need assistance to understand their cyber risks. To gain any form of management buy in, the risks need to be supported by actual loss information. Senior managers may think no loss = no risk, so what is the problem?

Governments, regulators, industry forums, businesses, and customers all require that eBusiness processes and technology be adequately and accurately audited for propriety, resilience, and accuracy. Many strategic and operational decisions are made using information generated by, or completely dependent upon, highly complex, interconnected, and devolved IT systems. Company officers seek assurance that there are sufficient controls in place to ensure the availability and integrity of this computer-dependent information.

We must also realize and accept our responsibilities for the fact that many commercial organizations are part of, or linked to, the national critical infrastructure. Many transnational organizations operate national water supply systems and gas or oil storage / delivery and electricity delivery. Often not seen as part of the critical infrastructure, but actually now have a considerable role to play, are transportation, banking and finance and telecommunications (including the Internet). This is in addition to the emergency services and Government operations.

The market has reached a point where the early adopters have learned first-hand the risks involved; some have had success, but many have suffered and have withdrawn. The second wave of companies, who watched the early adopters, have revised their plans accordingly. They have recognized the complex environment and are now seeking a resolution to the identified issues. Most importantly, they see the need for a real return on the investment in new technology, and will require that the range of risks identified be appropriately managed.

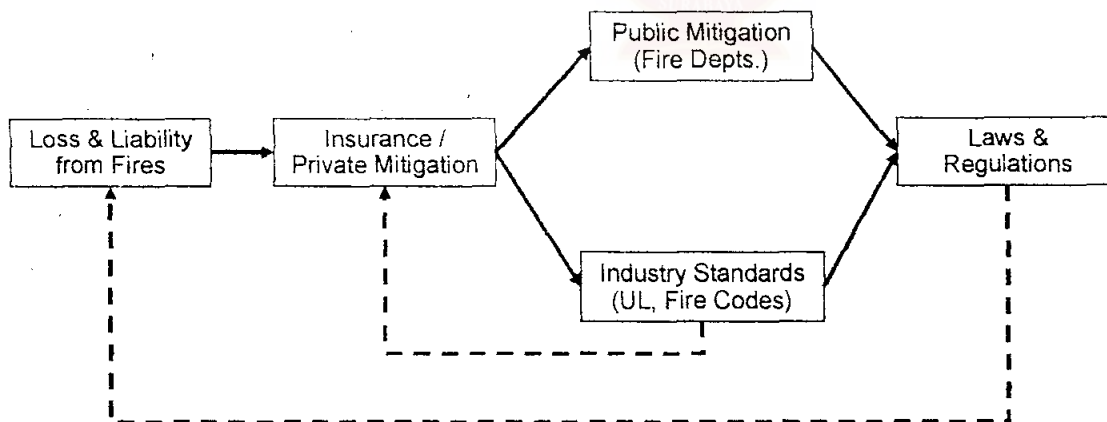# 5 Manage the Issues, but be Proactive and Enabling

A single infrastructure may have more than a million components if you consider the set of servers, network and communications devices, and associated software and firmware before you even begin to add the application data. These components may last more than 5 years and are supplied by multiple manufacturers. When you add the time for design, development, and replacement, it could take up to 8 years to replace an infrastructure even assuming there were enough trained engineers. Therefore, fundamental change will take years.

Building security into the infrastructure requires that every engineer involved must be aware at every step and therefore must be appropriately trained. When you begin to consider the low number of university graduates trained to design secure architectures and implement them using certified secure processes, add this to the previous paragraph for development and implementation, infrastructures are likely to remain insecure and threats will at best, remain constant for some 10 - 15 years. Education is key and an essential driver for change if we are to reduce this time lag.

It has become increasingly difficult to identify boundaries of responsibility, especially due to the complexity of systems and the range of risks. Not all are technical, though many IT security vendors will argue they have "*the* technical solution for all your needs". Players now include some or all of, commercial managers, security managers, lawyers, network managers, etc. The approach to understanding the threats and vulnerabilities now needs to become multi-disciplinary due to the interconnectedness of all enterprises.

The predominant view of security is a 'Police Department' model stemming from military and law enforcement where the focus is on defining criminal activity, catching criminals, and punishing criminals. It does some, but very little, to prevent crime. Information loss prevention is like fire loss prevention. You need to take a large view considering both the kind of loss and kind of prevention. Loss may be accidental (of operator or system), natural disaster, or criminal. Prevention relates to preventing fires from starting, preventing fires from spreading, and to limit potential loss when they do start and spread. Security solutions are stuck in the law enforcement-like thinking; we should, instead, adopt an active loss prevention mindset.

The 'Fire Department' model describes how, in the U.S.A., the local Fire Department carries the responsibility for enforcing the safe construction of buildings (from the fire prevention viewpoint). A brief history illustrating the development of insurance, standards, laws and regulations aimed at Fire Prevention is below:

Figure 1 – Progress towards Fire Prevention

In the past, there was little concern about the ability of a building to withstand a fire. However, materials were developed that provided improved resistance to fires. Technical standards were

created for these materials and they were required to carry a certification mark on them. This certification process was then communicated throughout the building community, so construction managers could easily check that components fulfilled the building requirements. Then there came a move to only allow buildings to be created from these new materials. Similar models are used in most countries. Ultimately, materials began carrying a safety rating and a safety mark. Test and certification processes were developed for the various materials.

Modern fire safety codes and standards[2] trace their origins to the nineteenth-century development of automatic sprinklers. From the beginning, sprinklers performed properly as extinguishing devices; however, they were originally installed in so many ways that their reliability was uncertain. In March of 1895, a small group of men representing sprinkler and fire insurance interests gathered in Boston to discuss these inconsistencies. They knew that nine radically different standards for piping size and sprinkler spacing could be found within 100 miles of the City of Boston. They realized that this plumber's nightmare had to be resolved or the rate of sprinkler system failure might prove unacceptable.

Building inspectors were trained in how the materials were to be used and how they should be placed within a building for maximum effect. They go into buildings under construction to verify the requirements are being met. The objective of all this effort was threefold:

- To prevent fires starting.

- To prevent fires spreading, thereby reducing the risk of a building burning down and to give the occupants more time to escape.

- To limit the potential loss when fires do start and spread.

An important consequence was to allow owners and constructors to show that they had taken all the required steps to prevent such loss in the event of the building burning down or loss of life. This last point has particular importance to the IT analogy, since the courts will inspect a company's actions to ensure they have implemented the best-known practice to prevent loss. It should be noted that in the automotive industry, health and safety follow a similar model.

The Fire Prevention Model is an excellent goal but one should view the analogy with an awareness of the differences. These differences do not negate the analogy; more they set a challenge in considering Information Security and Active Loss Prevention in a new perspective. It would be easy to say the analogy does not work, when accepting the challenge will help to identify a way forward. With fire, losses are largely due to accident and it is a fact that it is harder to insure against arson and lightning. With cybercrime, losses are generally due to deliberate action (hence no actuarial basis) and terrorists are not a probability distribution. It should not be forgotten that other incidents are also due to deliberate action, even if they are not malicious and may result from a lack of training or personal capability.

Fire resistance of material can be quantified (sort of), but there are no metrics for security. Perhaps because no vendor will accept liability and sells software almost "as is". It is not in their interest to make claims. The fundamental science of fireproofing and structural engineering is known and standards-based tests are available. The fundamental science of cybersecurity is not known. Fire damage is generally visible, but damage to information systems is often invisible. Standardization in fire prevention is advantageous when failures can be uncorrelated. Even fundamental aspects such as fire hose connections to hydrants were not initially standardized. Technical standardization in the IT world can be similar to a monoculture and introduce a weakness in the face of a correlated threat. Finally, the impact of fixes can be localized with regard to fire prevention, but due to the complexity of information systems, the impact of a fix there is often impossible to be localized.

---

[2] History of the NFPA Codes and Standards-Making System

6 Active Loss Prevention Requires Education and a Cross-Discipline Approach

Instead of the present, piecemeal, technology-driven approach to eBusiness and information systems security, it is necessary to bring together commercial, professional, and technology disciplines to create and drive the adoption of verifiable standards of eBusiness best practice. These standards will meet legal, audit, insurance, accounting, commercial, and governance requirements in the same way as other critical areas – financial, environmental, fire protection, automobiles, health and safety, and product liability. The Open Group has created the Active Loss Prevention initiative, which aims to get eBusiness and information systems risk and trust on to the boardroom and corporate responsibility agenda. Active Loss Prevention mirrors the philosophy used to protect buildings from fire worldwide – using codes of practice, standards, tests, laws and insurance to reduce the risk of fire, reduce its spread, and minimize damage when it does occur.

Research by The Open Group with 40 organizations from the US and Europe, identified issues and ideas for action that need to be taken and these have been incorporated into a program of work where organizations are directly involved in projects of interest to them. They will lead to improvements in the management of risk in eBusiness through Active Loss Prevention.

6.1 The Vision of Active Loss Prevention

The vision for Active Loss Prevention is to create an environment where eBusiness can flourish despite the risks inherent with using the Internet and other open communications. The environment will provide the infrastructure to create sustainable and trustable relationships between business partners.

From this vision, The Open Group expects to see the development of new standards and best practices. Some will be developed within the initiative, others by either specialized standards bodies or professional bodies.

As new standards or best practices are developed within the Active Loss Prevention initiative, there will be a requirement for promotion and education to help the standards become adopted in business at large. Any business engaging in eBusiness will need to use the tools and techniques developed by the initiative and other bodies. This will result in companies creating a new focus on loss prevention and risk management.

Following the "Fire Department Model", approved "Building Codes", approved designs and architectures, using certified components with approved construction and on-going use processes that could be adopted by organizations. Once in place, each business transaction can be controlled by a "traffic light", enabling business rules to be set; no-go, decision to be made or unrestricted. A key objective of making it simple for the user of the application must be followed.

6.2 Active Loss Prevention initiative

The IT model within organizations is out of balance with technology in the driving seat.

"The high-tech industry has inadvertently put programmers and engineers in charge, so their hard-to-use engineering culture dominates. Despite appearances, business executives are simply not the ones in control of the high-tech industry. It is the engineers who are running the show. In our rush to accept the many benefits of the silicon chip, we have abdicated our responsibilities. *We have let the inmates run the asylum[3].*"

In contrast, the Fire Department Model has evolved into a situation where the technology is relatively stable and the processes work. There are still occasional glitches, but the processes are in place to resolve them.

---

[3] The Inmates are Running the Asylum; Alan Cooper, SAMS, A division of Macmillan Computer Publishing; 1999

There is a set of aspects to be considered within the model. These are illustrated in the diagram below, together with an indication of the relative progress in resolving each one in each model. The IT model is the incomplete one on the left and the Fire Department is the (virtually) complete one on the right.

The Active Loss Prevention initiative intends to enable the transition from the IT model is to where it needs to be. To achieve this requires the involvement of all parties, as none of the aspects can be adequately resolved in isolation.

Involves all parties
(solving the business issues)

Technology relatively stable,
processes work

Enable the transition from where we are
now to where we need to be

Figure 2 - Illustration of the transition that will be enabled by the Active Loss Prevention initiative

It is to be a focal point for the translation of business requirements into technical requirements, but technical requirements that integrate well into the overall needs of business. The Active Loss Prevention initiative will contain a reference point for all parties and support them in such a way that all parties can identify the context of their position within overall business processes.

From the beginning, it is well understood that the initiative is ambitious. There will be no quick fixes. It is intended the projects identified so far are the first steps along a path that will take a number of years. Organizations that have committed understand this and they commit to a specific project or projects. This includes both a financial commitment and a commitment to providing resource. However, the benefits are significant as the Active Loss Prevention initiative is the only arena available where all disciplines work together to achieve a common goal.

6.3 Standards for Possible Solutions

It is often assumed that most solutions will be technology-based. However, by establishing cross-disciplinary teams, solutions can be developed that include the required legal and insurance elements as well. All standards must be underpinned by a clear business need and provide:

- A common means of communicating liability information;

- A common means of measuring or describing trust information;

- A means of communicating trust information (and the rationale behind it);

- A common means of describing the security status or risk profile of a system(s) and its connectivity (operating system, patches applied, applications, etc.);

- A common means of describing what security practices are followed;

- A means of communicating risk management information;

- A means of testing/evaluating the effectiveness of any or all of the above.

Standards will also need to include business and commercial processes and procedures, not just technical components.

6.4 Enforcement

Without enforcement, it will be difficult to ensure Active Loss Prevention. To achieve this, there should be:

- Common agreement on when to regulate and when to use self-regulation;

- Worldwide commonality on regulation, enforcement, and redress;

- Improved technical capability of law enforcement and regulators;

- Certification and supporting testing.

6.5 Education

Education is extremely important to achieve the vision of Active Loss Prevention for the following reasons:

- There are serious skill shortages (technical security and in the management of change) in the public and private sectors; and

- There is widespread lack of understanding, awareness and knowledge of good practice in organizations from the Board of Directors downwards; and

- Any new standard or approach to communicating trust must be understood by all participants involved, therefore it is likely that the initiative will sponsor some form of education program.

It is necessary to produce collateral for awareness campaigns, to promote speaking engagements and to develop self-teach modules for staff.

6.6 From Reactive to Proactive

This list is not exhaustive. The Active Loss Prevention initiative will discuss the issues and bring out other problems that need solving, and then initiate collaborative work to deliver new ideas and approaches to building tomorrow's infrastructure.

The concerns felt by senior business managers about the many risks they face in an increasingly hostile marketplace are very real. Risk management and loss prevention solutions must be focused on the needs of the business, using all forms of defense in an integrated and cost-effective manner to comply with relevant standards and best working practice. This is not being done at present, and there are many areas of risk that are being inadequately addressed and incorporated into business strategies that are normal in other business areas.

The Open Group's Active Loss Prevention initiative is intended to lead the transition from a reactive world, where we react to problems as they occur, to one where problems are anticipated, identified, and addressed before damage is caused. History teaches some valuable lessons and we ignore them at our peril. Active Loss Prevention looks at the needs of a business, how it communicates with other businesses, and what infrastructure is needed to support this business interchange. Therefore, the initiative must look at some basic issues such as trust, confidentiality, risk, and risk management. There are many overlapping areas of interest in the professional bodies that we will involve in the evolution of this initiative. One of the key features of this initiative is that these diverse interests will be brought together in a forum to create or adopt the necessary standards and guidelines.

7 How this can be Achieved

7.1 Principles of Active Loss Prevention

Active Loss Prevention, when fully and effectively implemented, will provide a number of elements. It will enable a Corporation to provide appropriate protection for all its assets in a cost-effective and efficient manner, addressing evolving threats in a coordinated manner. It will ensure an environment where all staff members are committed to the protection of the Company's assets and understand how to do that, treating eBusiness and all information and systems with the same concern given to financial and other more tangible assets. Competitive advantage will accrue through efficient and effective allocation of resources, and through the company's ability to seize opportunities effectively, because they know how to work with risk. It will contribute measurement and compliance techniques to identify and assess losses (including those resulting from breaches of IT security) and treat them in a fiscally sound manner.

Active Loss Prevention must follow some important principles. It must:

- Always be business-focused, and under business divisions' ownership and enforcement

- Strive to contribute business value ("enabling security to contribute") and provide best value for money

- Integrate all elements of risk management, security, people, processes, and technology

- Be an ongoing process, and not a one-off event

- Become part of the corporate culture

- Utilize other organizations' knowledge and experiences, to save time, money, and effort

- Deliver obvious early improvements to help gain and maintain support at all levels

The Active Loss Prevention initiative will use a variety of approaches and disciplines to address the issues of risk management. These approaches include the creation of appropriate test and certification programs and the identification and/or development of "technical" standards, relevant to risk management. It will provide a framework for the definition of the business problems that eBusiness causes, and define the requirements for tools that vendors of eBusiness products must provide to solve these problems. Also it will provide a framework for the definition of the rules, codes of conduct, and other related concepts that can be developed (involving *all* the parties that need a solution). Finally, it will take the initiative in promoting new operational and software tools and techniques.

The initiative has, for the first time, drawn together into the discussion all professions – lawyers, risk managers, insurance professionals, security specialists, auditors, investigators, and human resource managers – from private and Government sectors. The reasons all these people recognized the need to get together are to be found in the complexity of the problems to be overcome as described above. Working together, they will define the problems, consider solutions, develop standards and guidelines, and raise awareness about all Active Loss Prevention components. One of the overriding objectives will be to create information and best practice deliverables of immediate value to participants while building the long-term structure, products, and standards of Active Loss Prevention.

7.2 Managing the Active Loss Prevention initiative

The diagram at Figure 3 below illustrates the scope of the initiative and an indication of the currently identified projects. Broken lines represent the undefined aspects. Indeed, the whole program is undefined at present as the Active Loss Prevention initiative will grow and adapt through experience.

With an initiative having a program of this size and scope, it is essential that there is a project steering board; this group will provide the guidance for the overall project. This is described as a steering

group. It is also obvious that as this project progresses from its business perspective; it will need to both liaise and drive some technical projects. This group will be called the technology liaison group.
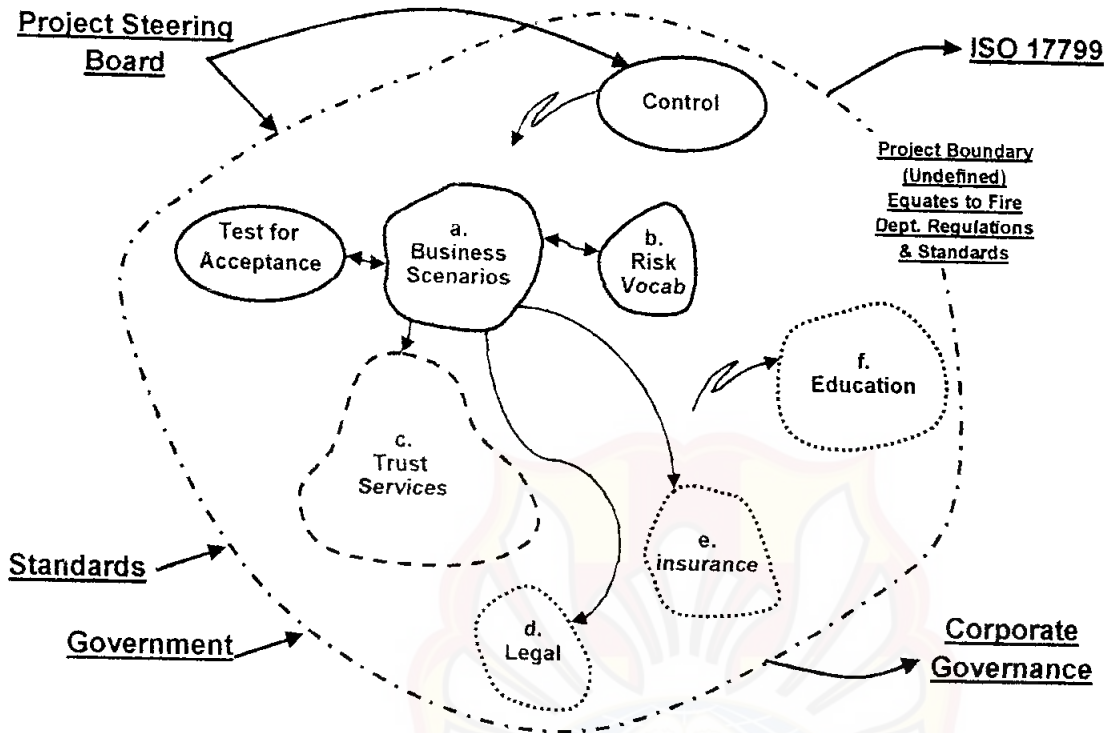

Figure 3 - Scope of the Program for the Active Loss Prevention initiative

It is intended to build on business scenarios in order to put the work within the Active Loss Prevention initiative into a context that can be understood and enables a common framework for review. A methodology has been proposed which links business scenarios through analysis to functional requirements, which in turn, will lead to technical, legal, insurance or other solutions. Ideally these scenarios will identify common business processes as well as identifying specific vertical market business processes. It is, however, intended to develop a common taxonomy of functional requirements for solutions to manage risk. These functional requirements will be linked to the Vocabulary of Risk and to Trust Services and other control measures.

Because technology and particularly information technology has such a large impact on business, a working group should investigate the strengths and weaknesses of current and new technology, to see when and where new action is required by the other projects.

7.3 Outline Description of Projects within the Program

From meetings and subsequent discussions, the projects that show the highest priority are:

7.3.1 Vocabulary of risk terms

Defining a vocabulary for the words associated with risk in the IT enabled business world is an urgent requirement. During the first Active Loss Prevention initiative meeting, it became clear that despite best efforts to date, there are significant uses of wording that have different implications to lawyers, insurers and auditors. This project is the first to start and is already gathering significant support in the legal, audit and insurance worlds. The deliverable from this method will be a word and phrase dictionary.

given environment. The IT industry will be able to create products or services that communicate these terms in standard ways.

The initiative requires a normalized set of risk terms, to reduce the risk of misunderstanding in communicating risk information between different professions. The agreed terms will make it easier to create standards for communicating risk information.

There are two distinct parts to the project: defining the scope and detail of the problem; and the creation of the terms and consensus building for their inclusion on the normalized terms

7.3.2   Liability

This project is an umbrella project for several anticipated projects. It will scope out the needs for standard contract terms, model law, model regulation, negotiation terms, standard terms of business etc. Each of the previous points could become a project, since there is much information gathering to be done and analysis of the data to lead to appropriate recommendations. The overall project could define where it is appropriate to create an IT solution to the business need and where process is needed. This group may also highlight areas where the IT industry must agree to self regulates itself. Areas where standards may be considered are illustrated in the diagram at Figure 4 below:
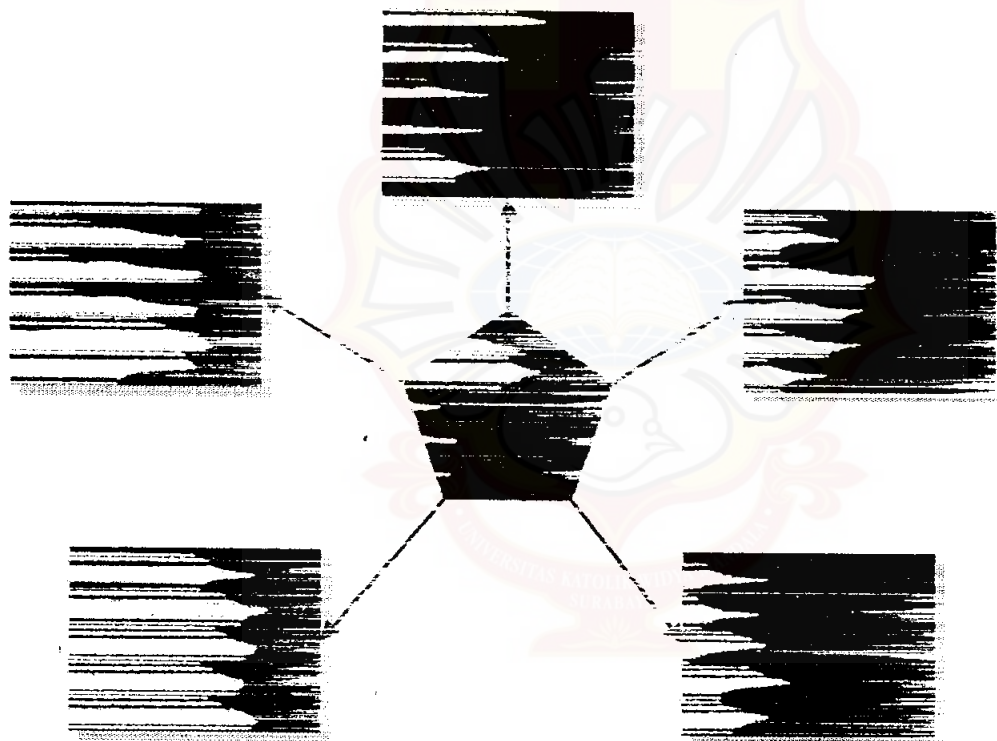

Figure 4 - Areas where Legal Standards may be considered

The initiative has identified that an inability to define where liability lies in an eBusiness transaction is likely to become an impediment to the future growth of eBusiness. The inability to assign liability clearly is already causing legal issues for some service providers.

There are two distinct parts to the project: defining the scope and detail of the problem; and the creation and management of the sub projects
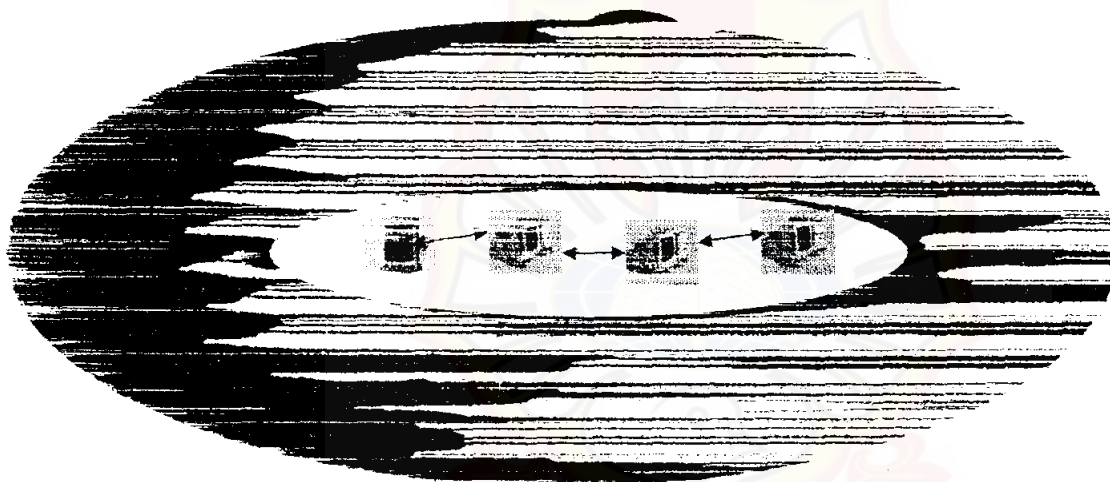
7.3.3   Actuarial data

This project will define the data that the insurance industry will need to gather in order to build actuarial data, assigning frequency, severity and normalizing the data across industries.

This data could be gathered and communicated in standardized components. These components are likely to be delivered to and from the underlying trust services (see below).

It is essential that the hype and over exaggerated impact seen in the press over the last couple of years is turned in to hard facts. This will require organizations to work together to deliver anonymised information about the impact caused by specific IT risks being exploited.

7.3.4   Trust services

This is a more technical group that will look at the underlying technical services that are needed to deliver the requirements coming out of the other projects. It is already possible to outline many of the services that will be needed in the future (illustrated at Figure 5 below). A large number of them are already in use, though not in any integrated form (perhaps not even in digital form). Given the size and complexity of some of the problems, we should start to work with the technology providers to define the most likely services that will be needed and to define how they need enhancing to meet the early outputs from the business led requirements. There are already clearly defined needs from the legal community that some trust services must provide (and do not). The objective of the trust services project is to ensure that the relevant business requirements are fed to the trust service providers and then tested against the business requirements.

Figure 5 - Trust Services

The initiative has identified the need for many trust services. These services can be defined from our current understanding of the general business requirements. They will be augmented as the requirements evolve. The services need some definition before work can start on the interfaces between the services. These interfaces are vital to the future usage of the trust services. Note that defining the interfaces will enable the technology vendors to innovate, at the same time create stability in the operational environment.

There are three distinct parts to the project: defining the scope and detail of the problem; defining what information is required to pass from one service to another; and the creation and management of the sub projects.

7.3.5   Education

This project will identify the set of subjects and target audiences where education is required. Understanding this will enable the development of appropriate awareness campaigns, speaking engagements and self-teach modules that can be deployed to promote Active Loss Prevention.

8   Conclusion

Adopting Active Loss Prevention will allow enterprises to be recognized as trustworthy and reliable business partners. They will benefit in two ways: by the reduction of losses and business advantage through security and process failures, and by increasing business and profitability as B2B and B2C customers gain confidence in doing business on-line and business partners reduce the cost of assuring each other's systems.

Realizing the vision of Active Loss Prevention requires a partnership between all the players – commercial, technology, and professional – in a trusted environment where good practices and standards and the means of verification and enforcement can be identified or created.

The inaugural Members of the initiative have committed to begin. Tarlo Lyons has agreed to sponsor the first project on developing the Risk Vocabulary and HP Research Laboratories have initiated work on the Trust Services. The project plans for both these projects are in development.

With a worldwide reputation in bringing together suppliers, buyers, and professionals, The Open Group has launched the Active Loss Prevention initiative and invites participation from organizations who see the benefits of Active Loss Prevention and want to gain by contributing, learning, and applying new practices in their own and their customers' businesses.

FRUIT PACKING AND STORAGE LOSS PREVENTION GUIDELINES

Prepared for Marsh Advantage and Wausau Insurance Company
by Anne M. Swindeman, Apple Advice, Yakima, WA.

INTRODUCTION

Every year fruit losses occur at warehouses that could have been easily prevented had communications or quality control programs been better. The information contained in this manual was compiled from many industry and research sources to help storage operators prevent fruit storage and postharvest chemical injury losses and the resulting insurance claims.

PREHARVEST CONSIDERATIONS

Controlled Atmosphere Equipment and Room Preparation

Each facility should have a lead storage operator who is properly trained and certified in refrigeration technology, preferably with a good working knowledge of the fruit industry. In addition, a maintenance contract should be in place with a reputable refrigeration service.

All controlled atmosphere (CA) rooms should be leak tested by competent personnel every year prior to loading. All leaks should be repaired until the room is sufficiently tight. Floor bumpers should be installed if not already present. This is also a good time to disinfect walls, refresh floor striping, install and calibrate temperature probes and service refrigeration equipment. Analytical equipment should be calibrated and oxygen and carbon dioxide cells should be replaced by certified technicians. A working, calibrated portable analyzer should be on hand to serve as a back up to the main analyzer.

Safety inspections of the facility should also be made. If corridors or mezzanine walks are present within CA facilities, sample tubing should be in place so oxygen and ammonia levels can be monitored to ensure worker safety at all times. Signs should be posted outside of all CA rooms clearly warning of the danger of low oxygen within the rooms. Compressor rooms should be posted with "Authorized Personnel" signs.

All maintenance procedures should be recorded in a dedicated book. This book should be preserved for historical purposes.

Marketing and Harvest Strategies

Proper harvest maturity is absolutely critical for the successful storage of fruit. Since ideal harvest maturity is dependent on the intended destination of the fruit, marketing plans should be discussed in detail with the field staff during the preharvest season. These plans will determine the amount of fruit needed for each storage regime and marketing period throughout the year. The field staff should also be expected to communicate any delays or horticultural concerns as they occur since these may change the overall plan.

Drench and other postharvest chemical applications should be outlined as well. Pears are extremely susceptible to scald, so the marketing plan should be designed to ensure that pears are treated with ethoxyquin very soon after harvest. If they are not to be drenched upon receiving, packing line time should be made available within a short time of harvest to prevent both scald and scuffing.

Certain apple varieties such as Granny Smith should have an antioxidant treatment such as diphenylamine (DPA), regardless of storage regime. DPA is optional for short term Red Delicious, Gala, Fuji, and Braeburn since these varieties are not highly prone to storage scald; the latter two varieties may benefit from DPA if internal browning is a concern that growing season. These varieties may benefit from calcium (particularly when spring weather is cool and calcium uptake is low) and fungicidal drenches regardless. This is the time to evaluate market demands and consult with growers if this is a grower option at your warehouse.

MCP (SmartFresh™, AgroFresh) is a newly available postharvest tool for apples. We may find that it will replace the need for DPA on certain varieties; however, there is a lot about this chemical that we do not yet know. It significantly reduces fruit respiration; therefore, it appears not to be a viable product for use on apples having watercore at harvest. Internal browning disorders may result if applied to watercored apples. Therefore, SmartFresh is not currently recommended for use on Fuji, Braeburn and late harvested Red Delicious with watercore. **As with any chemical, always follow the label!**

Orchard Sampling

A proper sampling program ensures that representative fruit is tested within each block. For determining fruit maturity, non-damaged fruit from average, as well as **more advanced** maturity should be the focus for testing since the primary goal is to prevent condition problems and other related disorders in storage. At least 10 fruit should be collected and tested from each sampling location within an orchard block. Locations to sample should include the earliest area of the orchard block, an average area, and the latest area of the block if at all possible. Undamaged fruit should be harvested from the south or west side of the tree and outer 12 inches of canopy. These will represent the most mature fruit of each location. Factors such as bloom date, soil type and tree vigor may be of help to the field staff or consultant in determining these areas. Preharvest maturity testing should begin in the orchard on a regular basis at least 2 to 3 weeks prior to anticipated harvest, depending on the commodity.

Maturity Testing

Pears are harvested pre-climacteric with respect to ethylene production, meaning they have not yet begun to ripen on the tree. Two highly informative articles written by Paul Chen and Diane Varga can be found at the end of this manual.

Bartlett harvest is usually started when average firmness approaches 18 lb, depending on fruit size. Larger fruit will be generally less firm than smaller fruit at the same maturity level due to cell size differences. If ethylene testing is available, ideal maturity of Bartlett would correlate to 3 to 5 days before onset of the ethylene climacteric. Properly harvested Bartletts should store well in CA for up to 3 months and retain normal ripening capacity.

Anjou pears are harvested typically 2 or more weeks preclimacteric, at approximately 135 to 147 days, or when firmness levels approach 15 lb. At this time, the lenticels begin to cork and the flesh color between the lenticels lightens, wax develops and the fruit becomes rounder as it fills out. Soluble solids measurements and starch tests are also of additional value in determining Anjou maturity. Due to the number of postharvest maladies affecting Anjou pears stored long term, most rooms should be targeted for opening within six months of harvest.

Harvesting too early results in greater susceptibility to storage scald, friction marking (scuffing), and inability to ripen properly. Harvest for shorter term storage can generally be delayed until firmness is approaching 13 lb. Harvesting later may result in yellower fruit with a reduced storage life, and an increased susceptibility to carbon dioxide injury. Firmness measurements on pears are most representative if done in the morning hours.

Apples are optimally harvested at a mature, yet pre-climacteric state with respect to ethylene production for long term CA storage, and post-climacteric for the shorter term CA storage regimes. At a minimum, fruit firmness and starch iodine tests should be done with results recorded on each sample weekly by experienced personnel.

Ethylene monitoring is recommended on apples destined for long-term CA storage, since successful storage is highly dependent on harvesting fruit prior to the onset of the ethylene climacteric. This onset of ethylene production precedes significant firmness and starch changes. The optimum harvest window for truly long term CA storage may be as short at 3 days in some orchard blocks.

Firmness varies from grower to grower and variety to variety. Orchard nutrition programs and fruit size play significant roles in firmness as measured in preclimacteric fruit. Therefore, some fruit may be mature at 18 lb, whereas other fruit may not be mature until it is 13 lb. Most export and many domestic buyers are currently demanding 14 lb and higher Red Delicious, and there are minimum firmness requirements in place for several varieties in the Washington apple industry.

Starch charts are available for each major apple variety and there are recommendations available from extension specialists regarding trends. However, just as firmness can vary with growing conditions, so can starch measurements. Starch is converted to sugar as fruit respire. Fruit with a high nitrogen to calcium ratio respire more rapidly than nutritionally balanced fruit. Fruit grown in hot seasons will respire more rapidly than in cool seasons. Fruit treated with ReTain (TM, Valent BioSciences), a growth regulator that delays ripening processes for up to 2 to 3 weeks, will tend to have higher starch ratings than non-treated fruit at full maturity (ethylene onset) due to the fact that respiratory processes continue during this time.

Soluble solids (sugars) should be used to a minor degree, if only to reference flavor development. Nutrition programs, crop load and maturity all influence soluble solids, so there are no absolute values available to use in maturity determinations.

It is important to note that even the best controlled atmosphere technology will not reverse the ripening processes if fruit is harvested too late or mishandled after harvest; fruit harvested too late will result in condition problems, increased potential for storage rots and other internal disorders. Harvesting too early, on the other hand, can lead to the development of superficial storage scald, bitter pit and/or poor flavor development.

HARVEST AND STORAGE

Warehouse Receiving, Sampling and Testing
Fruit should be delivered to the warehouse, sampled for quality control purposes, drenched (if applicable), and put under refrigeration as quickly as possible after harvest. This should be done within a day of harvest since ripening processes occur at a much higher rate once fruit is detached from the tree. If for some reason the warehouse cannot receive the fruit quickly, it is

much better to delay harvest. The possible exceptions to this rule are Braeburn and Fuji (as long as the weather is cooperative), since these varieties seem to benefit from added ventilation and slower cooling.

Samples should be pulled from each load of fruit upon delivery to the warehouse, except in the case of very large lots in which case sampling every second or third load may suffice. These samples should then be tested for firmness, starch and soluble solids and all data should be recorded for future reference. The actual number of fruit tested should be representative of the quantities delivered. For a full load of 64 bins, it is recommended that at least 15 to 20 undamaged apples of a representative size range be selected and tested from the load. At the same time as receiving samples are pulled, samples may also be conveniently pulled which will later serve as "window" samples in the CA room (see "Pulling Window Samples" below).

Pulling Window Samples
Enough fruit should be pulled from loads being received so that at least 10 fruit (preferably 15 to 20) from each lot can be tested each month from the CA room. Some warehouses place these samples into boxes designated for each lot. All samples are kept cold during the receiving process, and upon filling the CA room, monthly samples may either be pre-bagged at random from the composite sample or the entire box may be placed at the CA room window. This will result in a more representative sample of fruit across the room than bagging samples from particular loads or harvest dates.

Be aware that using poly bags for samples can create false atmospheres (higher carbon dioxide, etc.) so samples may not be truly representative of the fruit actually stored in the bins if temperatures are allowed to fluctuate. Samples must be handled similar to the incoming bins in order to be truly representative.

Drenching
Always follow label directions! Do not try to stretch drench chemicals as contamination with spores and debris can cause further fruit damage. Have a testing program in place to monitor chemical concentrations accurately on a regular basis; some chemical dealers also sample fruit at regular intervals for laboratory testing.

Ethoxyquin should be applied to Anjou pears either as a postharvest drench and/or at packing, depending on storage regime and fruit maturity. Split applications are permissible, as long as the total amount does not exceed the current label. Regardless of the method of application, **it should be noted that ethoxyquin is most effective as an antioxidant if applied no later than one week after harvest.**

In general, apples destined for CA storage for over 3 months should be drenched with DPA and fungicide (usually TBZ), unless it is organic. Calcium drenches are recommended in certain varieties such as Jonagold and Golden Delicious, both prone to bitter pit. In hot growing years and years with cool springs, calcium drenches can significantly increase fruit calcium levels and help prevent storage disorders from occurring.

Storage Compatibility of Varieties
Fruit of the same variety or of compatible varieties should be stored together whenever possible, with the exception being for short term rooms. Golden Delicious and Jonagold apples are high ethylene producers in CA, often producing values as high as 1,500 to 2,000 ppm in static rooms

(rooms using lime). Red Delicious, Rome, Braeburn, Granny Smith and Pink Lady® brand apples are moderate ethylene producers, generally producing in the 200 to 500 ppm range. Gala ethylene production tends to slow down once under CA, and Fujis tend to be low producers throughout; these varieties generally test below 200 ppm. Nitrogen purged and carbon scrubbed (dynamic CA) rooms generally have only ~10% of the ethylene levels as lime (static) rooms.

Anjou pears are very low producers of ethylene and are extremely sensitive to ethylene. Bartlett and Bosc will produce rather high levels of ethylene once ripening begins. **Because of these differences, all rooms should be isolated by valves as soon as possible after pulldown to prevent gas mixing (including ethylene) between rooms.**

With the exception of Braeburn, Granny Smith, Fuji and Pink Lady® brand rooms (see Table 1), CA rooms should be filled and sealed within 3 to 7 days of harvest. Oxygen pulldown in apple rooms should commence as soon as a fruit temperature of 50 °F or lower is reached. **Delays in oxygen pulldown of 2 weeks or longer are not acceptable for most varieties.**

Table 1. CA storage recommendations.

Variety	Antioxidant concentration	Cooling rate*	Temp. (°F)	Oxygen (%)	CO₂ (%)	O₂ pulldown rate*
Anjou pears (long term)	Ethoxyquin, up to 2700 ppm	Rapid	31.5 to 32 °F	1.5 to 2.0%	< 0.5%	Rapid
Anjou pears (short term)	Ethoxyquin in wraps	Rapid	31.5 to 32 °F	0.5% 1st month 1.0% 2nd month then to 1.5%	< 0.5%	Rapid
Gala	DPA, 1000 ppm optional	Rapid	33 to 34 °F	1.0 to 1.5%	< 2.5%	Rapid
Red Delicious (long term)	DPA, 2000 ppm	Rapid	32 °F	1.2 to 1.5%	< 2.5%	Rapid
Red Delicious (watercore)	DPA, 2000 ppm	Rapid	32 °F	2.0 to 2.5%	< 2.5%	Moderate
Golden Delicious	Optional	Rapid	33 to 34 °F	1.2 to 1.5%	< 2.5%	Rapid
Jonagold	Optional	Rapid	33 to 34 °F	1.5%	< 2.5%	Rapid
Granny Smith	DPA, 2000 ppm	Rapid	34 °F	1.5%	< 1.0%	Slow
Braeburn	DPA, 1000 ppm optional	Stepwise	38/36/34 °F	1.5 to 2.5%**	< 1.0%	Slow
Fuji	DPA, 1000 ppm optional	Stepwise	38/36/34 °F	1.5 to 2.5%**	< 1.0%	Slow
Pink Lady® brand	DPA, 1000 ppm	Slow	33 to 34 °F	1.8 to 2.0%	< 1.0%	Slow

* Cooling and O₂ pulldown rates:
  Rapid = within 3 days
  Slow = 5 to 7 days
  Stepwise = 36 to 38 °F during loading, 36 °F at sealing, 34 °F after 2 to 3 weeks of CA establishment

** Watercored fruit should be stored at elevated oxygen levels (2.0 to 2.5%) to prevent anaerobiosis and internal breakdown.

(from Apple Advice, revised 2002)

CA Room Loading, Sealing and Pulldown

CA rooms should be precooled to the desired setpoint before product loading begins. The porthole should be cracked during the precooling process to alleviate any sudden pressure changes in the room which could result in blown seals and/or structural damage to the CA room. Refrigeration equipment problems, if present, will often be revealed at this point.

All personnel involved in loading CA rooms should be instructed on proper loading techniques as well as forklift safety. Your warehouse should have a forklift safety program already in place. To ensure proper loading, floors should be lined out (striped) to make this process clear. Floor bumpers not only help with bin to wall spacing requirements for optimal air flow patterns, but also help reduce the incidence of wall damage during loading. Forklift drivers should understand the importance of reporting any possible damage that has occurred during the loading process. Only bins of the same size and type should be used to avoid air circulation problems which may result in fruit losses. If bin types must be mixed, a gap should be left between the types so that air flow can be redirected into the bin runners appropriately. Be sure to leave a free space of 18 to 24 inches at the front and back walls.

In the case of static CA rooms, drivers should be instructed as to amount and placement of pallets of lime within the room. The amount of lime used should be sufficient to last the entire anticipated storage period; typically for mid to late term storage, 2 lb per box should be allotted. More lime should be used if growing conditions were unfavorable (cool springs, excessively hot summer/fall weather). If fruit nitrogen to calcium levels are out of balance (too much nitrogen), lime needs may be higher since respiration rates tend to be higher in this type of fruit. **Lime is required if there is no other means available to scrub (remove) respiratory carbon dioxide.**

Pears should be moved from the orchard to the storage within 24 hours after harvest. Rapid removal of field heat is essential for successful storage of pears. Pears should be completely precooled prior to oxygen pulldown. Fruit should be cooled to 30 °F within 5 days of harvest. CA conditions should be introduced as soon as possible as any delay following harvest reduces postharvest life and fruit quality. Low oxygen (0.5% oxygen) CA storage and dynamic (purge) CA systems are proving successful in scald prevention. See Chen articles (in Reference section) for further information.

Monitoring CA Rooms

Analytical equipment must be calibrated by trained personnel at the beginning of the storage season and at recommended intervals (more frequently if at all possible) with span gas. Many new analyzers recalibrate themselves continually. Alarm systems should be programmed to call several different persons in the case of emergency. Ammonia sensing cards are also available to place at the portholes for a quick reference and double check.

Even if your facility is fully computerized, it is a good practice to **manually check** each room weekly with a back up analyzer at the room portholes. This will help prevent storage losses due to failing oxygen and carbon dioxide sensors, improperly calibrated analyzers, power outages that have inadvertently reset parameters, sample lines which have been damaged, etc. All monitoring must be done by trained personnel to ensure accuracy of calibration and best use of information. Any discrepancies in data between monitoring equipment should be immediately noted and investigated. If ammonia sensing cards are used by the facility, this is a good time to check them as well.

CA rooms should be analyzed for temperature (preferably using multiple probes located in the rooms per the Mexico program), oxygen and carbon dioxide levels twice daily. Many computerized facilities are analyzing these parameters hourly, as well as monitoring for ammonia throughout the day.

There are times when the calculated amount of lime "runs out" before the operator is ready to open the room. In these cases, it has been found that raising the oxygen level to 1.0% above the carbon dioxide level will help prevent internal fruit damage.

Quality Control of CA Rooms

It is recommended to check fruit quality on a regular basis (usually monthly) within the CA rooms. Without these checks, it is nearly impossible to distinguish some chemical injuries from other disorders as time goes on. Knowing when the disorder first appears is often essential if the cause of the disorder is to be determined.

Most facilities begin testing window samples (samples pulled upon receiving from each grower lot) in early December. Window samples are most helpful in assessing storage disorders such as scald and internal browning if they are kept at ambient oxygen for at least one day prior to pressure testing. After making an initial visual assessment of the fruit, firmness measurements should be recorded, after which fruit should be cut to view internally and "feel" for condition weaknesses near the core area. Oftentimes, fruit firmness measurements (taken from the outer surface of the fruit) are misleading since some fruit will soften internally first; this is why a follow up "feel" is helpful. Whenever disorders are noted, either internally or externally, an investigation should be made as to the cause. More samples may need to be tested directly from bins in the room in order to determine if the damage is to a single grower lot or multiple lots within, and also if it is progressive. When looking at firmness measurements, both the average and range of values (standard deviation is helpful) should be taken into consideration each month. It is also helpful to record fruit size, color and "grade" of fruit within samples when recording data. Only packable fruit should be tested for firmness; culls should be noted but discarded.

Monthly ethylene monitoring of the CA atmosphere has also proven valuable in determining fruit condition. Sudden or significant increases in ethylene can alert operators to distressed fruit up to 2 months prior to actually measuring the increased rate of fruit softening. This flexibility allows a warehouse to open the CA earlier if possible and market it before condition is compromised.

Opening CA Rooms

Safety procedures should be in place regarding open CA rooms. Team approaches to opening rooms are best, in case of medical emergency. Extreme caution must be taken to prevent any human or animal from entering the CA room before it is adequately aired. Some facilities open the sampling door and place a cage over this door to hasten airing. Others stack empty bins closely in front of the door. High volume fans may help reduce the amount of time to air up a room.

Bruise-sensitive varieties such as Golden Delicious and Granny Smith often benefit from airing prior to packing. Many warehouses will open Golden rooms and allow them to sit for

approximately 3 days at slightly elevated storage temperatures (~40 °F). This allows for a slight dehydration of the skin which seems to help reduce bruising.

Hardier varieties can be unloaded from the storage as soon as the oxygen levels in the room have reached ambient conditions.

PACKING

Packing and Packed Fruit Storage

Less friction marking occurs on pears that are picked at the correct maturity (i.e., not immature) and packed within 3 to 4 weeks of harvest. When pears are packed directly from cold storage, do not warm prior to packing. Avoid unnecessary drying of pears as water lubricates the fruit on the packing line. Reducing the packing line speed is also effective in reducing injury.

Chemical injury is another major problem with pears. Fruit must be rinsed thoroughly after leaving the dump tank as the salts in the flotation solution can cause irreparable damage to the skin. Fruit should also be dry by the time they are wrapped in copper/ethoxyquin impregnated wraps to avoid marking.

Before each packing shift begins, dump tank water temperature as well as chlorine and fungicide concentrations (and pear float solutions) should be checked and adjustments made if needed. Make sure the wax type is correct for the variety or order being packed (for instance, Braeburn apples do not tolerate shellac waxes well). A daily log should be kept regarding all levels of chemicals and wax types used. Adhere to all state and federal laws.

Palletized fruit should be returned to refrigeration as soon after packing as possible. Refrigerated rooms should be loaded to enhance cooling of the packaged fruit. Pears and other ethylene sensitive commodities should not be stored in the same rooms as apples and other high ethylene producers unless pre-ripening is desired!

Packed inventory should be turned as quickly as possible, and a quality control person should make regular checks on packed inventory for condition changes.

EMERGENCY PLAN

A written emergency plan should be in effect for every warehouse in the event of injury, fires, chemical spills, ammonia leaks, etc. All employees should be provided with training to ensure that they understand procedures.

SUGGESTED READING/LIBRARY REFERENCE MATERIALS

Postharvest disorders of apples and pears. Agriculture Canada Publication 1737/E, 1994.

Market Diseases of Apples, Pears, and Quinces. Agriculture Handbook No. 376, USDA, 1971.
http://postharvest.tfrec.wsu.edu/market_diseases.html

Chen, Paul M. and Diane M. Varga. Storage Challenges with Winter Pears. In: Washington Tree Fruit Postharvest Conference Proceedings, 1996. p. 79-83.
http://postharvest.tfrec.wsu.edu/PC96A.pdf

Chen, Paul M. and Diane M. Varga. CA Regimes for Control of Superficial Scald of d'Anjou Pears. In: Washington Tree Fruit Postharvest Conference Proceedings, 1997. p. 17-26.
http://postharvest.tfrec.wsu.edu/pgDisplay.php?article=PC97A

Kupferman, Dr. Eugene. Observations on Harvest Maturity and Storage of Apples and Pears.
http://postharvest.tfrec.wsu.edu/EMK2000A.pdf