available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information Lifecycle Security Risk Assessment: A tool for closing security gaps

Ray Bernard

Ray Bernard Consulting Services, USA

Keywords:
Data lifecycle risk analysis
Electronic data security
Electronic document management
Enterprise data management
Information lifecycle security risk assessment
Information security risk assessment
Physical data security
Proprietary information protection
Records and information management

ABSTRACT

News media continue to report stories of critical information loss through physical means. Most information security programs include physical protection for information system infrastructure, but not for the physical (non-electronic) forms of the information itself. Thus organizations have persistent critical information vulnerabilities that are not addressed by even the most extensive of information systems security programs.

An *Information Lifecycle Security Risk Assessment*, as described in this paper, can be used to extend the reach of information security programs to encircle all forms of critical data from creation to destruction—even data in human memory form. Such an assessment can leverage existing data management and information systems security efforts. By incorporating both electronic and physical information elements, previously unaddressed information security gaps can be identified and mitigated. The end result should be a risk treatment plan which senior management can understand and approve, and which managers and security personnel can execute.

A high-tech manufacturing company pointed to a $10 million drop in service business revenue as evidence of substantial quality improvements in their product lines. An astute board member launched her own investigation and determined that the real cause was encroachment on the service business by competitors, who had been illegally obtaining physical copies of proprietary company information and for over two years, had been using it to quietly take over customer service accounts.

For over a year the largest sales branch of a national company experienced a level of sales competition unheard of in any other sales office, resulting in the lowest sales closing average in the company's history. Personnel from a competing company were sneaking up to the sales team's conference room window at night, and peering through tiny slots in the window blinds to copy the daily list of hottest sales prospects from the white board—including products and anticipated sales amounts.

While incidents of information loss by physical means of one kind or another are routinely reported by news media and security publications, many instances—like the two described above—are not publicly disclosed. For decades *Records and Information Management* (RIM) professionals have managed information in paper or other physical forms, and have utilized physical security programs to manage the protection of that information. Then how is it that today many critical information losses are the result of successful *physical* attacks? How is it that the protection of information in physical forms is poorly addressed in many organizations, despite the increased awareness of the importance of information protection?

1. Information security redefined

Today broadband networks and high-capacity electronic data storage technologies enable organizations and individuals

E-mail address: raybernard@go-rbcs.com
0167-4048/$ – see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.12.005

to create, receive, store, access and publish information in quantities—and at speeds and economies—that remain impossible with physical forms of data. Organizations have embraced electronic forms of information for their ability to accelerate the pace of any information-based activity. Electronic forms of data have substantially replaced physical forms of data for most organizations.

Thus in recent years several new phrases have replaced *Records and Information Management* in organizational parlance: *Electronic Document Management*, *Enterprise Data Management, Enterprise Content Management, Document Lifecycle Management* and most recently *Information Lifecycle Management*. Such approaches are concerned with the practice of applying policies to the effective management of information in all aspects of its useful life. These new approaches to data management reflect the migration from a physical to an electronic organizational data landscape.

However, unlike their predecessor, RIM, most of the solutions under these names have a common focus mainly or solely on the electronic aspects of data handling and storage. For most organizations critical data still exists in other forms, and their security is not addressed by the security components of the electronic data management approaches.

Information systems security practitioners are aware of the fact that the scope of their work is limited to electronic data. For example, the CISSP designation stands for Certified Information Systems Security Professional, where ''Information Systems'' means ''electronic data systems''.

In contrast, the well-known information security standard, ISO/IEC 17799:2005, states in its introduction:

> Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.
>
> Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Yet in everyday use the term *information security* is most often applied to *electronic* information security, the realm of IT security practitioners, where the application of physical security is limited to information systems physical infrastructure. This amounts to an unintentional redefinition of *information security*, causing vulnerabilities to many non-electronic forms of data to fall out of organizational view.

Another part of the picture is the fact that regardless of the inclusion of physical and environmental security in 17799 or any other information security standard, the vast majority of information security practitioners have neither the knowledge nor the means to implement physical security controls for non-electronic forms of data. For information security to be complete, all forms of data must be addressed, and they must be addressed by the personnel who have the knowledge and means to identify and mitigate their information security risks.

2. Infrastructure focus also afflicts physical security

A close focus on infrastructure also can be found with physical security practitioners. They attend to building external and internal structures, means of access (such as doors, windows, roof hatches, etc.) and physical facility vulnerabilities. Physical forms of information are protected in part as a side-effect of protecting the rooms that contain them, similar to how electronic information is protected in part by physical protection of information systems infrastructure. Outside of government and private sector facilities with classified information, in most companies many physical forms of information are not subject to sufficient security controls. The exceptions are generally those organizations that have suffered a physical loss of critical information, and have closed the open doors related to their loss events. Information is usually only loosely tied to physical protection zones, and that is done at the time that physical protective measures are initially established. As organizations change, their usage of information changes, and the physical forms of information and their locations change also. Yet physical protective measures are rarely reevaluated unless physical building structures change.

3. Need for a workable process

What is lacking is single a process whereby the critical information assets, *in all of their forms*, can be identified, cataloged, ranked in terms of their criticality,[1] and protected by establishing and maintaining suitable controls. The solution involves what is often referred to as *security convergence*: the collaboration between IT Security departments and Physical Security departments, groups which are historically separate functions in most organizations. To date what has helped to keep the two groups separate is their infrastructure focus, which takes them in different directions. What does enable the two groups to collaborate successfully is the *risk perspective*. It provides a common vision that makes a single process workable for both groups, and can encompass both physical and electronic forms of information. The information lifecycle approach provides a birth-to-grave scope that facilitates identifying all of the forms that information can take, electronic and physical. This results in an information risk assessment process that is truly complete in its scope.

4. Information security stakeholders

Collaboration between Physical Security and IT Security departments is only a starting point for an Information Lifecycle Security Risk Assessment. To be successful the risk assessment process must involve personnel outside of the security departments. Typical information security stakeholders include personnel from Human Resources, Legal,

[1] Criticality is the severity of impact of the loss of the asset.

Compliance, Audit, and Risk Management; but they can only provide part of the risk picture.

Users of the information in various business units understand its role in their critical functions, and the impact of its loss. They also know how information is accessed (not always in conformance with policy), what forms the information can take, and where physically the various forms of information can be located.

Managers who are responsible for the business units that depend on the information assets are information security stakeholders from several perspectives. First, they often make decisions about who can access information, and where. Second, they have a responsibility to see that the information assets on which they depend are safeguarded, and so require input into the security process at least in terms of identifying the critical assets. Third, they must also support and enforce security policy and controls within their own areas, which is an organizational responsibility. Fourth, sometimes security considerations warrant a change to a business processes—at times requiring the physical relocation of a business function that is not in a secure enough location. Such changes require not only management approval but also active management involvement to execute them successfully.

Additionally, senior management must be informed about and provide approval of major security initiatives. After all, the information assets are corporate assets—not the security departments' assets—and the decisions about what levels of risk to accept are not security department decisions. Security departments and security executives can and should make recommendations, but ultimately the decisions must rest with the senior executives who are responsible for the corporate assets, and with the executives who are responsible for success of the business units that depend on the assets. Thus senior executives are also information security stakeholders.

Generally senior managers usually do not understand all of the workings of security, but they do not need to. When presented with a good risk picture and prioritized risk treatment plan, they can easily weigh the cost of risk reduction measures against the potential impact of risk events on the business. This information allows them to become security advocates for the assets they are responsible for or on which they depend. Strictly speaking this is not an advocacy on behalf of security; it is an advocacy on behalf of the business.

5. Collaboration strategy

The strategy proven to be most successful for fully addressing the critical information risk picture is one that involves all of the stakeholders: an *Information Security Risk Management Council*, a group whose actual name will vary (task force, committee, etc.) depending upon the organization. Such a council can fulfill its role when its members can speak to the full lifecycles of the critical information assets, either by their own direct involvement or by survey and discussion with those who are directly involved. Early in its work a council may discover that its members cannot adequately address the full lifecycle of all of the critical information assets. It is usually a simple matter to expand the membership slightly to achieve that coverage. Typically the council includes members from Human Resources, Legal, Compliance, Audit, Risk Management, IT Security, Physical Security, Corporate Security, and the organization's various business units. The council may report to the CIO, the CEO, the CFO, or to whichever senior executive volunteers for or is assigned top-level oversight. There are usually dotted line reports as well.

6. Information lifecycle

The roles or functions involved in information handling constitute key aspects of the information lifecycle from an analysis perspective. They form a simple checklist that can help guide the effort to identify the various forms information can take:

- Creation and Receipt
- Storage
- Distribution and Transmittal
- Access and Use
- Maintenance
- Disposition and Destruction

Creation and Receipt deal with records from their point of internal origination or their entry into the organization. Information forms can be written, printed, electronic or verbal and include correspondence, contracts, applications, reports, drawings, production or transaction records, and many other forms of data.

Storage refers to all of the places where any form of information is stored, including human memory.

Distribution and Transmittal are processes involved in getting the information to locations where it can be accessed and used. This may happen automatically according to some process or policy, or on request or demand.

Access and Use take place after information is distributed, and may involve converting the data from one form to another, such as printing reports or documents for review, and information sharing on an individual or group basis.

Maintenance is the management of information. This can include processes such as information filing, archiving, retrieval and transfers, as well as changing the classification of information as its value, relevance or validity changes.

Disposition and Destruction involve handling information that is rarely accessed or is required to be retained in specific formats for specific time periods, and is then destroyed by appropriately secure means when it is no longer valuable or required to be retained.

In addition to helping identify the various forms that information can take, there is another beneficial aspect of the information lifecycle approach that pertains to security cost and efficiency. The value of some information changes over time and a lifecycle analysis can identify those change factors. It is good business practice, as well as good security practice, to adjust the level of resources used to safeguard information as the criticality of the information changes.

7. Information Lifecycle Security Risk Assessment

The first step of an Information Lifecycle Security Risk Assessment is to determine or identify:

- the full lifecycle of each operationally critical data asset (creation or receipt, storage, distribution and transmittal, access and use, maintenance, disposition and destruction);
- all the forms in which the data can exist at each point during its lifecycle;
- all the physical locations at which each form can be found or produced;
- what corporate security policies and procedures exist (if any) regarding the various forms of data in each location;
- what personnel (internal and external) can possibly access the data, regardless of whether or not such access would violate any policies that may exist; and
- the effectiveness of any security measures being applied, including inspections and audits.

This provides a baseline picture that can be used to perform a risk analysis and develop a prioritized list of cost-effective measures that should be applied to each data asset during its lifecycle. The remaining risk analysis steps can follow whatever qualitative or quantitative risk analysis methodology is most applicable for the organization. Risk analysis recommendations should include the categories of items shown in Table 1.

An important final step is to update the ongoing information systems risk management program to include periodic checks for changes to each data asset's lifecycle. Change management should trigger reassessment whenever a critical data asset's lifecycle changes.

8. Protecting physical forms of data

Ironically it is the migration away from physical forms of data to electronic forms that makes securing physical forms of information much easier today than it has been in the past. These are some of the reasons:

- Regulations (like Sarbanes–Oxley and HIPAA) require deployment of physical security measures; this is a new driver for physical security.
- Publicized instances of physical loss of critical information have educated senior management to the real dangers of physical security gaps.
- The information security programs and business continuity plans of many organizations have cataloged the critical information assets and provide a significant head-start in the identification of electronic and physical forms of critical information.
- The information classification schemes of enterprise data management programs can be used for the physical forms of information as well, significantly reducing the preparation effort involved in cataloging physical instances of information.
- The framework of an information security management system, such as what ISO/IEC 27001:2005 defines, can also be utilized to establish and maintain physical information security as an incremental effort to existing information systems security management.
- Role Based Access Control implemented for information systems access can be extended to physical access control systems (PACS), either through manual processes and procedures or via integration with an Identity Management System or corporate directory. This provides a way to include physical forms of data in policy-based management of information access, which can be a boon to compliance management

9. Human protective measures

There are some forms of data that can only be protected by appealing to their human custodians. Where information exists in human memory form, security measures like non-disclosure agreements, internal disclosure policies, and

Table 1 – Recommendation categories

Recommendation	Example or explanatory note
Security strategies	Example strategy: for each form that a data asset can take in its lifecycle and for each location where the data form can exist, ensure that a specific person or role is assigned responsibility for the data asset's protection.
Security policies	Policies determine what protective actions are taken when, where and by whom.
Security procedures	Specific and standard steps that implement the actions required by security policies.
Compliance monitoring	Implement compliance monitoring as appropriate by IT security, physical security, or audit department depending upon the security measures to be monitored.
Corporate safeguards	Where significant corporate liabilities exist, institute measures that help safeguard the corporation, for example: forensics quality recorded video surveillance or adjusted insurance coverage.

security awareness training apply. Individual personnel briefings should be utilized when personnel are terminated or transferred, to provide a reminder about information protection obligations that continue despite leaving the organization or some part of it. Some forms of information—like data on PDAs, cell phones and notebook computers, as well as printed information—require safeguarding by the person who has their custody.

Smart card based security systems, especially those which incorporate biometric authentication for critical data, can provide a secure bridge from system to human custody, by controlling the transfer of electronic data into physical form. Printing solutions (such as FollowMe® Printing, Follow & Print, and Cardn'n'Print) exist that require the authorized individual to present a security card and/or a fingerprint at the destination printer before controlled documents will actually print. By applying policies about where sensitive data are allowed and not allowed, printer selection can be restricted by printer location based upon the classification of the data being printed, as well as by the security privilege of the individual printing the information.

Similar restrictions can be applied to writing data to a disc or memory stick, to provide auditable physical chain-of-custody control as information is transferred to a portable medium.

10. Lifecycle approach advantages

One advantage of the lifecycle approach is that it can be applied to any security risk assessment methodology. Its function is to provide a process for the identification of the all of the various forms of information that require protection, which fits into the asset identification step of any information risk assessment methodology. Another advantage that is unique to this approach is that it constitutes a simple point of collaboration in which all security stakeholders can participate, thus providing a bridge between corporate, physical and IT security participants regarding information protection.

Ray Bernard is a security consultant and a writer, who has provided pivotal direction and education in the security profession and the security and building controls industries for more than 20 years. He is the most highly published writer on the subject of the convergence of physical convergence and IT, with more than two dozen full-length feature articles on the subject in a number of security trade publications, in addition to a monthly column, ''Convergence Q&A'', in *Security Technology & Design* magazine. He is a frequent presenter at security conferences and workshops, and conducts a full-day security convergence track each year at the *CardTech-SecurTech* conference. His security consulting clients include Fortune 500 companies, international airports, and critical government and public facilities. Additionally he is the founder of ''The Security Minute'' electronic newsletter, the first newsletter for all security stakeholders. Bernard is also certified as a *Physical Security Professional* (PSP) by ASIS International, and holds the Certified in Homeland Security *CHS-III* designation from the American College of Forensic Examiners Institute (ACFEI).