Protecting Aggregated Data

US-CERT

December 5, 2005

Produced by US-CERT, a government organization

Table of Contents

Executive Summary

In their ongoing quest for improved operational efficiency, organizations have come to rely on the ability to collect, access, and process large volumes of electronic data (aggregated data). This reliance has evolved with the development of sophisticated database software and the growing availability of hardware with storage capacity measured in terabytes. By possessing such large volumes of data, however, organizations assume certain risks and responsibilities:

- Large data stores are valuable informational assets that have become targets for cyber criminals.
- Electronic data can be easily copied, modified, and distributed, making the total retrieval or destruction of compromised or stolen data assets impossible to confirm.
- Owners and custodians of large data stores assume responsibility for maintaining the privacy and integrity of the information under their control.

Theft or compromise of customer, partner, or other data held by an organization has a number of short- and long-term consequences. The dollar value of these consequences can exceed that of the data itself. These consequences include

- interference with an organization’s day-to-day operations
- interference with an organization’s ability to fulfill customer and partner transactions
- erosion of trust relationships between the organization and its customers and/or partners
- violation of federal and/or state laws governing the protection of aggregated data
- exposure to civil litigation claims

By applying sound management principles and good security practices, organizations can mitigate these risks and better protect the aggregated data under their control. Organizations must understand the nature and disposition of the data, determine its value, and calculate acceptable risk. Their data management and security strategies must make leaders accountable for effective oversight of data security, heighten data security awareness, ensure legal compliance, and require regular data security audits and the development and execution of incident management plans. Leaders and the strategies they develop should also address sound security architecture and design, physical security management, the management of partner processes and activities that affect data security, vulnerability management, and business continuity. By working to ensure the security of the aggregated data in their charge, organizations can not only avoid the negative consequences associated with a data security breach, but strengthen their relationships with customers and partners and enhance their reputations in the community at large.

Purpose and Scope

The purpose of this paper is to discuss the security issues, business impacts, and potential strategies of U.S. industry, government, and academic organizations that create and maintain large aggregations of data, such as digital repositories, databases, data warehouses, and aggregated information systems. The paper first examines characteristics of data and information with respect to how they create security management challenges when information is compiled and aggregated. The paper highlights consequences, negative impacts and ramifications to organizations, partners, and users due to data compromise including manipulations, disruptions, disclosures, thefts, and loss. Finally, the paper discusses effective security management approaches and strategies to address the issues and to mitigate risks.

Background

Organizations and information security staff are facing an increasing number of attacks against mass stores of their customer, private, and sensitive information. All of us have read the headlines identifying corporations, universities, and government agencies that have lost control of their database records to attackers. The growing list of attackers and methods of attack against such data stores is real and has the potential to negatively impact business, government, academia, consumers, and the citizenry.

At the center of the attacks are the common databases, repositories, and data warehouses required to conduct operations in the public and private sectors. Because of the decreasing cost in storage devices and the increasing desire for business intelligence and analytics, enormous volumes of electronic information are being aggregated and, consequently, placed at risk. For instance, two years ago, information-technology-oriented media outlets were writing articles describing only a handful of the largest commercial databases pushing 75 terabytes in size [Orzech 03]. Today, similar articles talk of these sizes as commonplace, where the typical organization’s database ranges between hundreds of gigabytes to tens of terabytes [Mearian 05]. How big is this? Consider that 1 terabyte of electronic data is equivalent to 50,000 trees worth of printed paper [Berkeley 00].

The term data aggregation refers to the trend toward amassing, preserving, and using large volumes of electronic information. Organizations engaged in data aggregation may do so for any number of reasons, including archiving, analysis, and operations. Aggregated data also includes the metadata needed to index, flag, define, or access the information, as well as the content itself. The volumes of this type of data are most often amassed into an electronic repository without regard to their logical or physical structure, and are generally free from organizational compartmentalization that results from the physical and operational requirements of the people who interact with them. Aggregated data is most often found and described by the technology that houses it, such as a database, data repository, storage array, file system, or data warehouse.

The risks posed to aggregated data are numerous and derive from both external and internal threats, such as natural disasters, failures of internal controls, sabotage, and attacks. This paper is concerned with aggregated data security as it pertains to losses due to attackers that are external to the organization that is responsible for managing the aggregated data. The following scenario describes this problem:

A database containing 100,000 records for current and past students at a large university in the northeast was attacked by unknown parties on the Internet. The compromised data contained admissions, health, academic transcript, disciplinary action, residency, housing, student employment, and emergency contact information. The school's response was to warn current students and alumni of the risks posed to them by their information being possibly copied and stolen. They claimed the potential for misuse of some or all of their information could include identity theft and financial fraud. They instructed the victims to keep a watchful eye on their credit reports. The university stated that they were investigating the incident in an attempt to prevent this type of problem in the future.

If we hold it to be true that "information is the lifeblood of an organization" we must also recognize the significance of our information resources, such as volumes of aggregated data. This significance is amplified by the desire of attackers to exploit these resources for their gain and our need to routinely transfer, store, and process these resources to conduct business, government affairs, etc. Customers, users, and stakeholders demand increasingly more privacy and protection for the information they provide to organizations in return for products and services. They place confidence in organizations to perform effective enterprise security management and understand the risks not only to an organization's sensitive data but to a customer's private information. They expect these risks to be managed regardless of where the information is stored, transmitted, or processed, be it internal to the organization or through partnerships. This customer focus is sometimes lost in the mass of multi-terabyte databases of aggregated data.

Understanding the Problem

When archivists look to preserve information, they understand that the media serves the content, not vice-versa. Hence, the content drives the retention standard and policy, not the storage media, be it paper, microfiche, or tape. Similarly, in information security it is the content that drives the security requirements and information systems that serve to fulfill these requirements. In organizations' attempts to secure information (the content), they need to consider that the systems where the information resides are a target of attacks and thus a key concern for information protection activities.

In large database systems, the content is a compilation of aggregated data. As much as databases lend themselves to supporting organizational processes, they also make clear targets for attacks: one-stop shopping locations for information thieves. The problems associated with databases are not the structure of information; they lie more with the characteristics of electronic information, especially aggregated data. Problems also stem from aggregating data in one or a few logical locations and the potential for loss of control, in use, and ownership. This section briefly explores some of these problems and issues.

Replication and Persistence

When left unprotected, aggregated data can be easily replicated, shared, altered, and destroyed. When a physical object is created, such as a car, it exists until it is completely consumed or becomes obsolete. In either case, the final disposition is that the object is destroyed and ceases to exist.

This same characteristic should apply to volumes of aggregated data. The exception is the ease with which information can be replicated at any point during its lifetime. This creates a potential situation where information cannot be disposed of easily due to the proliferation of copies. Worse yet, aggregated data, in electronic form, can exist past the point of obsolescence, persisting in perpetuity.

Ownership

Another set of characteristics describe ownership and custodianship of aggregated data. Continuing the analogy with a physical object, the identification of who owns and operates a car is usually bounded and well understood. We know two things: first, that a car has a title, its ownership is documented, and there is a defined process for transferring ownership. Second, mechanics who service the car maintain it, but do not own it. In contrast, aggregated data rarely has a well-defined title of ownership. Aggregated data is constantly changing in both ownership and custodianship because of the ease with which electronic information is shared, transferred, and replicated. For example, each time a piece of information is used in conjunction with other information, it is likely that the owner and custodian are different. Here, owners are the proprietors of an organizational process using aggregated data while custodians are the users and administrators of the technology used to access the aggregated data.

Transformation

Aggregated data undergoes a constant transformation. Information by definition is “the communication or reception of knowledge or intelligence [Webster 05].” For our purposes, data is processed, analyzed, and aggregated to produce information. The transformation of data into information occurs because organizations use raw data in the aggregate and within a given context, yielding information and intelligence.

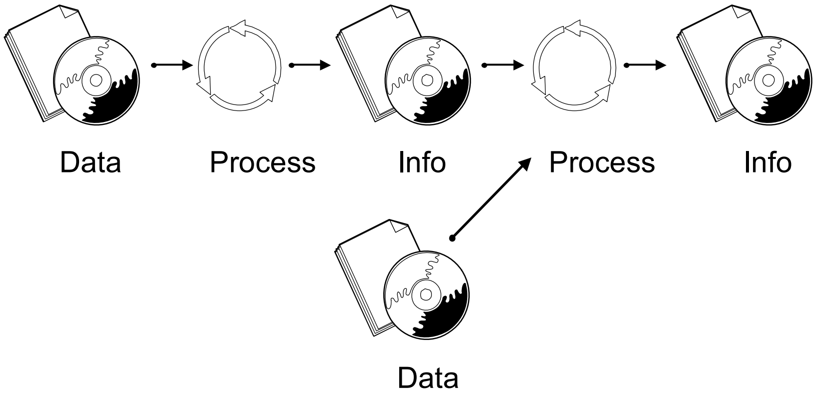

Figure 1: The Information Cycle

The continual cycle of moving sets of data through a process that creates information (see Figure 1) presents challenges for determining clear ownership of aggregated data and the information from which it derives. Data from different sources is often combined to create new information. This is an important problem for intangible assets like aggregated data, as a clear boundary for the asset and its ownership is required before its value can be determined. Value is key to determining the level of investment for protection strategies.

Valuation

Valuing information of any type has proven to be difficult for most organizations. Information assets are not often carried on the books as capital assets, so determining a monetary value is not straightforward. Often, the value of an information asset is found in the process it supports and not in the information itself. The value of the aggregated data to an organization can only be determined if the person or persons responsible for the organizational process it supports understand and agree on exactly what is being valued.

Aggregated data often has many owners, users, and custodians. This creates situations where the exact value (or even an approximate, relative value) of the aggregated data is difficult to calculate. Determining the value is an attempt to capture how important the aggregated data is to the organization. Data value derives primarily from its use, but organizations need to also consider the impact of its loss or unavailability. Valuing aggregated data, taking into account its unique characteristics, is critical for determining the risks, the impacts, and thus the necessary investments in protection strategies and security actions to adequately protect such data.

Understanding the Risks and Impacts

Consider what it costs you if

- customer data is compromised and it makes the headlines
- your brand and reputation are negatively affected by a data-related security breach, resulting in a loss of customer confidence and loyalty
- sensitive intellectual property (such as government or trade secrets and new product information) is stolen by a competitor or made public
- your organization is found to be non-compliant with privacy and data protection/reporting regulations (international, national, state, local)
- your network goes down because of a data compromise
- you can’t detect a data compromise

The risks associated with managing aggregated and sensitive data in electronic form and with network access are many. Organizations often find themselves in the position of custodian for critical sensitive information belonging to others who trust the organization to handle this information responsibly. Reciprocally, owners assign responsibility for protection to custodians; this demands that owners communicate security requirements explicitly and ensure custodians meet the established requirements.

Determining the range of actions an organization needs to take to reduce aggregated data security risk to an adequate or acceptable level depends on what an organization needs to protect and what it needs to prevent. Consider the following questions:

- What responsibility do we have for protecting the information in our computer systems, particularly information that belongs to others? What needs to be protected? Why does it need to be protected? What happens if it is not protected?
- What are our worst-case scenarios for security compromise? Most likely scenarios? What potential adverse conditions and consequences need to be prevented? At what cost?
- How much disruption can we stand before we take action?
- How do we determine and effectively manage residual risk (the risk remaining after mitigation actions are taken)?

The answers to these questions can help organizations determine how much to invest, where to invest, and how fast to invest in data protection. They serve as one means to identify security risks to aggregated data and quantify the degree of risk exposure. In the absence of answers to these questions (and a process for periodically reviewing and updating them), an organization may find it difficult to define and deploy an effective aggregated data security strategy and thus unable to effectively sustain an adequate level of protection.

Value Placed at Risk

Organizational 'assets' that can be negatively affected if aggregated data security is inadequate, performed poorly, or compromised include

- trust
- customer and partner identity and privacy
- the ability to offer and fulfill customer transactions
- the ability to meet compliance, legal, and regulatory requirements

Organizations can experience an immediate impact in the short term as a result of a compromise of aggregated data security, and impacts can be realized in the longer term. Aspects of each asset and impacts to them are described in the following sections.

Short-term Impacts

Ability to Offer and Fulfill Customer Transactions

The Internet has equalized access to information and aggregated data world wide. Risks and opportunities increasingly derive from who you are connected to and who is connected to you, rather than from where you are physically located. Because of the ready and direct access customers have to those with whom they wish to transact business, and the ease with which they can change these choices for any reason, customers drive today's marketplace.

An organization's ability (or inability) to competently offer and fulfill customer transactions is most visible to the customer. This includes a customer's profile, preferences, and historical buying habits, often stored in aggregated databases. In the case of commercial business, making items of interest easy to find, with accurate and competitive pricing, with immediate order confirmation, and with timely delivery contribute to the growth of Internet-based business. Online banking provides a good example of how aggregated data security enables customer transactions. Bank customers are typically assured of identity and privacy protection with respect to their personal information, transaction histories, and a secure flow of funds via an Internet connection. Imagine how this changes if the customer's data is compromised and this is publicly reported. Imagine what the impact would be if the entire roster of customers were negatively affected by a security breach of the bank's volume of aggregated customer account data.

The ability to lower transaction costs (discovery, negotiation, arbitrage, settlement, and adjudication) depends on electronically accessible and aggregated data. The Internet and the electronic commerce it enables have lowered transaction costs compared with predecessor technologies. However, the nature of electronic communication is that it is location-independent, essentially instantaneous, and—unless modified—anonymous [Geer 04]. These qualities introduce new risks to aggregated data that must be taken into account by organizations owning and serving as custodians for such data.

Customer and Partner Identity and Privacy

Concerns about the risks associated with personal privacy and identity are growing. Violations of these type and their costs, legal consequences, and effects on reputation are regularly reported in the media. A typical example states, "The Federal Trade Commission estimates that approximately 3,000,000 Americans were the victims of identify theft in 2002. A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information-security and privacy practices" [Braun 04]. Disclosure of personal information entrusted to an organization can have a profound impact on that organization's reputation.

As identity theft and related violations of privacy become more prevalent, public backlash from both customers and legislators could be significant. Increasingly, customers and organizational partners expect a certain standard of aggregated data security practice from any competent organization. This expected standard is likely to continue to escalate. However, reputation need not be considered solely in negative terms. Leaders should also ask, "How much is it worth for us to be seen by our customers and partners to be actively concerned with safeguarding their information?" Proactive approaches to security can enhance an organization's reputation as a trusted partner [Charette 05].

International privacy regulations, such as those in the European Union (EU), Japan, and Australia, are more stringent than their U.S. counterparts, so approaches to comply with such regulations must be developed with proper appreciation of country or regional requirements. Given greater customer privacy concerns, data protection authorities in several countries are most concerned with protecting healthcare, pharmaceutical, and financial services data [Gartner 04].

U.S. or multinational organizations should be especially wary of how they treat EU employee data and how they monitor EU employees' electronic activities. EU employee tribunals are common, and EU employees frequently take their employers to court.

Increasingly, organizations are finding that a global approach to privacy can meet the majority of national or regional privacy requirements, providing some opportunity for cost containment through standardization.

Almost all organizations collect, process, store, disseminate, and transfer customer information in some form, most likely digital. Protecting such information and preventing actions that can cause unintended disclosure and use are increasingly required to meet legal requirements and preserve customer trust.

Long-term Impacts

Trust

Achieving and preserving trust are among the most essential outcomes of protected aggregated data. Trust is an element of protecting customers and their information, protecting market share, sustaining market and customer confidence, preserving reputation, and enhancing an organization's brand and image. Trust is hard to build and easy to lose in the face of a public breach of security or customer privacy. Just consider companies enjoying headline attention as their customer databases are compromised, raising widespread concerns about identity theft. Some are finding that regaining trust once it is lost may not be possible.

An increasing number of organizations understand the inextricable link between trust and securing aggregated data in today's globally connected environment. One CISO states "Security is a necessary consideration in everything that we do. We need to protect customers and employees. We are the custodian for a lot of information that belongs to other people."

Compliance and Legal Liability

Failure to protect stakeholder interests with respect to certain categories of information or failure to prevent unauthorized access to personal information may have serious legal consequences. A comprehensive approach to protecting aggregated data can help an organization maintain compliance with new and expanding laws and regulations and avoid legal liability related to statutory or common law.

Rather than focusing on a framework for cyber or information security, current U.S. federal legislation and related regulatory programs have focused on an interest in either of the following:

- protecting the privacy of individually identifiable information held on private computer systems
- improving private-sector oversight of financial reporting

Three current U.S. laws need to be considered when addressing responsibilities to protect aggregated data:

- the U.S. Gramm-Leach-Bliley Act of 1999 (protecting personal information for financial-institution customers)
- the U.S. Health Insurance Portability and Accountability Act of 1996 (protecting personally identifiable health information held by certain entities)
- the U.S. Sarbanes-Oxley Act of 2002 (mandating expanded public-company financial-control audits, including information security)

These laws have all provided regulatory incentives for senior-level managers and oversight agencies (such as boards of directors and trustees) to pay closer attention to information security, including the protection of customer privacy and identity. A similar security effect derives from both state and international law. The California Database Protection Act (CA SB 1386 (notification of personal security-information breaches) and European Union (EU) Directives on data protection and privacy and electronic communications are affecting multi-state and multinational organizations [CRS 05]. Consideration for extending aspects of the California law to all U.S. states is in progress.

Compliance issues related to legislative and regulatory programs and the criminal and civil liabilities that can arise from their violation are only one part of the legal-liability exposure. There remains the significant liability that can result from national/federal and state court litigation claims based on a breach of contract, tort, or property rights. Civil litigation provides an effective platform for the promotion of individual privacy and identity protection. Such litigation might drive the adoption of standards governing security controls on aggregated data.

Security Management for Large Volumes of Aggregated Data

Understand the Information

The first step in protecting anything is to understand it. For aggregated data, this entails understanding what information exists, where it exists, and in what form. Determining an adequate level of protection also requires knowing the security requirements, owners and custodians, and potential risks and impacts. Once the basic information is known about large volumes of aggregated data, the data can be broken into smaller units and profiled.

Profiling, or the process of describing, categorizing, and bounding information, is one way to understand the unique characteristics and protection requirements of information. In this case, a smaller and more manageable set of aggregated data is used for profiling. Owners use profiling techniques to explicitly and unambiguously define:

- information descriptions and boundaries
- designations of owners, custodians, and users
- information security requirements, such as access and authentication requirements of users
- logical and physical locations where the information is stored, transported, and processed
- information value and sensitivity

Owners must know the value of their information to develop a meaningful profile. Such a profile is used by custodians to select appropriate security controls to protect the information. The owner of the information asset and its stakeholders determine the value of the information to the enterprise or organizational unit. The contribution of the information to the owner's goal achievement (or the potential to impede goal achievement) is reflected in the valuation. One way to consider the value of an asset is to look at the potential impact on the organization (and the owner) if something were to happen to it.

A significant amount of guidance has been issued to help federal government agencies determine and assign value to their information and information systems. Federal Information Processing Standard (FIPS) Publication 199 and National Institute of Standards and Technology (NIST) Special Publication 800-60 provide explicit guidance. Information value is determined by looking at the potential impact on the organization if the security of the information is compromised. Information is first classified by type (public relations information, for example). Then for each type of information the potential impact is rated on a high, medium, or low value scale for each security objective, which NIST defines as the triad of confidentiality, integrity, and availability.

Every organization needs to determine its own approach to and process for information valuation. Once the value of the information and the degree to which risks and impacts can negatively affect it are known, an organization can develop a meaningful profile against which to apply management and security controls to mitigate risks and manage impacts.

Apply Good Management Principles

A good set of commonly accepted management principles aids an organization's leaders in determining what protection strategies are best applied to secure aggregated data. Organizations can use principles to select, interpret, prioritize, deploy, and reinforce policies, strategies, plans, actions, and expected behaviors. To be effective and of greatest value, principle selection and interpretation should align with organizational objectives including the requirement to protect sensitive aggregated data.

The following principles apply to protecting and securing aggregated data. These are briefly described in this section :

- Accountability
- Adequacy
- Awareness
- Compliance
- Measurement
- Response
- Risk Management

Each of the principles is stated using the present tense, conveying what actions, behaviors, and conditions demonstrate the presence of the principle in the organization's culture and conduct.

Accountability: Organizational leaders are accountable for providing effective oversight of aggregated data security, including ensuring effective execution of the agreed-to protection strategies. Such accountability and responsibility are explicit, defined, acknowledged, and accompanied by the authority to act. Leadership accountability and responsibility for aggregated data security are visible to all stakeholders.

Leaders possess the necessary knowledge, skills, and abilities to fulfill these responsibilities. Individual roles, responsibilities, authorities, and accountabilities are assigned. Leaders ensure that all users with access to aggregated data understand their responsibilities with respect to this access. Leaders conduct regular evaluations of their aggregated data security program, review the evaluation results, and report on performance to oversight authorities, including a plan for remedial action to rectify any deficiencies.

For example, one area reviewed and reported on would be data retention policy and procedure. Leaders work with aggregated data owners and custodians to ensure processes are documented, implemented, and secure for purging data when the need or requirement to maintain the data has expired.

Adequacy: Investment in aggregated data protection strategies (principles, policies, procedures, processes, controls) is commensurate with risk. Determination of risk is based on the value, sensitivity, and criticality of such data with respect to its vulnerability to loss, damage, disclosure, or denied/interrupted access. Probability, frequency, and severity of potential vulnerabilities are considered. Leaders ensure that sufficient resources (people, time, equipment, facilities, dollars) are authorized and allocated to achieve and sustain an adequate level of aggregated data security.

For example, leaders ensure data owners and custodians work together to understand the compartmentalization that sensitive aggregated data sets require. Leaders use policies to direct owners to declare value and identify security requirements (confidentiality, availability, integrity, and authentication) and direct custodians to implement sound and measurable security controls.

Awareness: Leaders are aware of and understand the need to protect aggregated data. They understand what actions are necessary to protect stakeholder value with respect to such data. All users are aware of aggregated data security risks and protection strategies and understand their concomitant roles and responsibilities. Awareness is demonstrated by the motivation, training, and education provided to users who are given access to sensitive aggregated data and by attendance at periodic training as a requirement of continued access. Performance reviews include an evaluation of how well these responsibilities are fulfilled.

Compliance: Aggregated data protection strategies are in compliance with legal and regulatory requirements, requirements of conducting business, and requirements established by external stakeholders. Actions necessary to evaluate compliance objectively (such as internal and external audits) are built into the security compliance program. This includes regular monitoring, review, and reporting of compliance findings to affected and interested parties. Leaders ensure that remedial and timely action is taken for any aggregated data security deficiencies.

Measurement: Leaders identify and request periodic reports on measures and indicators that demonstrate the value and adequacy (or lack thereof) of aggregated data security protection strategies. “What gets measured gets done. Metrics are about transforming policy into action and measuring performance. Metrics indicate how well policies and processes are functioning and whether or not they are producing desired performance outcomes [CISWG 04b].”

Response: All users (including leaders) act in a timely, coordinated manner to prevent or respond to threats to aggregated data security and compromises of it. Such response requires development and regular exercise of business-continuity, disaster-recovery, crisis-management, and incident-management plans so that the enterprise is adequately prepared in the face of an attack and is able to resume normal operations as quickly as possible.

Risk Management: Leaders continually review, assess, and modify aggregated data security protection strategies in response to the dynamically changing risk environment in which they operate. Leaders articulate acceptable levels of risk to aggregated data assets based on their value, sensitivity, and criticality (see Adequacy). Such levels are examined during regular review and assessment processes.

Costs of compromise (loss, damage, disclosure, denied/interrupted access, costs to reconstitute) are quantified to the extent possible as part of ongoing risk management. Controls are selected to effectively mitigate risk and their performance is regularly measured and reviewed. Plans for remedial action to rectify risk-mitigation deficiencies are developed and executed following each assessment.

Apply Good Security Practices

As with management principles, a good set of commonly accepted security practices help an organization meet the protection requirements of aggregated data. Practice selection and adoption derive from the security strategy of an organization. Organizations use practices as they implement security policies, strategies, plans, and actions. To be effective and of greatest value, practices should guide control selection and address risk mitigation efforts necessary to adequately protect sensitive aggregated data.

The following practice areas apply to protecting and securing all types of information, including aggregated data. These are briefly described in this section:

- Information Security Strategy
- Information Security Policy
- Security Architecture and Design
- Incident Management
- Partner Management
- Contingency Planning and Disaster Recovery
- Physical Security Management
- Information Technology
- Audit and Monitoring
- Vulnerability Management

Each of the practice areas is stated using the present tense, conveying what actions, behaviors, and conditions demonstrate the presence of the practice in the organization’s culture and conduct.

Information Security Strategy: The security strategy is part of the organization’s overall strategic planning activity and serves as a systematic plan of action for implementing, maintaining, and improving the security posture of an organization. The strategy encompasses and describes the organization’s information security program, including all of the activities and processes that are performed to ensure the mission’s survivability. This includes the protection of aggregated data, considered in the context of all other security strategy actions. It considers the unique operating circumstances of the organization, as well as its culture, mission, and critical success factors. Effective security strategy aligns with, and supports, the business strategies and drivers of the organization.

Information Security Policy: An information security policy is the compilation of guiding principles the organization defines to establish the limits and boundaries of behaviors for using information resources and assets, including aggregated data. The core of the information security policy defines the organization’s risk tolerance, which is indicative of the range of security events the organization is prepared to withstand. For example, a higher risk tolerance may signify that the organization believes it would not suffer a significant or material impact if a security weakness or vulnerability is introduced and/or exploited. As the organization’s risk tolerance narrows, a more extensive security strategy is necessary as well as well-defined and prescribed guidelines for behavior and action.

Security Architecture and Design: Security architecture and design is the physical and logical implementation of the organization's security strategies, policies, and procedures. It is the organization's technical implementation of security structure throughout the various layers of the technical infrastructure. This includes physical devices, hardware, software, and the ways in which security is managed and administered in this infrastructure. Security architecture and design addresses the unique requirements reflected in the profile for each subset of aggregated data. This practice includes ensuring systems on which aggregated data is stored, processed, and transmitted are securely configured and that configurations are kept up to date using a well-defined and enforced change management process.

Incident Management: Incident management is the organization's process for identifying, reporting, and responding to suspected security incidents and violations, including those involving aggregated data. The organization is prepared for incidents involving the organization's network and technical infrastructure, physical facilities, and human resources, such as social engineering attempts. The organization's ability to address incidents as a part of the overall security strategy provides another tool for monitoring its environment, understanding what threat and vulnerabilities they are susceptible to, and to develop proactive mitigating and protective strategies. For aggregated data in particular, incident management includes the processes for required communication and notification of affected parties, such as customers. Incident management may also include remedial and corrective actions necessary to restore customer confidence.

Partner Management: Partner management processes and activities require that vendors and service providers act in ways that support the survivability of the parent organization. Organizations communicate to these partners what is important to the organization, and how they are expected to behave so that they do not expose the parent organization to further risk. Parent organizations recognize they ultimately retain responsibility for ensuring the tasks are completed and that the goals and objectives are achieved. It is essential that partner organizations understand their roles and responsibilities and are held contractually liable for adequately protecting aggregated data that is owned by the parent organization and for which the partner is a custodian or user.

Contingency Planning and Disaster Recovery: Contingency planning and disaster recovery direct the approaches and actions taken by the organization to continue normal operational functions when confronted with significant or adverse disruption. Contingency planning involves the proactive and reactive steps to facilitate an effective and efficient recovery from any contingency that puts the organization's mission at risk. Managing the impacts involves and requires appropriate policies, plans, and procedures to be documented, communicated, tested, and evaluated before a contingency situation occurs. Contingency planning and disaster recovery practices include ensuring aggregated data backups are regularly made, transmitted securely (encrypted), reach their backup storage location, are stored securely, and that aggregated data can be restored to a known state from any given backup media.

Physical Security Management: Physical security is a component of the comprehensive protection strategy, particularly for tangible aggregated data resources (such as hardware, software, and media). It compliments the organization's network and system security by physically protecting and acknowledging the logical instantiation of systems and network security controls.

Information Technology: Information technology security is the range of technical mechanisms that the organization deploys to enable and enforce policy, standards, and procedures. Technical practices and mechanisms are applied to counter known and anticipated threats and vulnerabilities to aggregated data, software, systems, and networks. In addition to threat avoidance, resistance, detection, and recovery, technology also supports security controls such as least privilege/separation of duties, access control, role-based authentication, firewalls including use of policy-segregated networks, change and patch management, aggregated database server configuration control, encryption, redundancy, adequate implementation of aggregated data profiles (including separating sensitive from non-sensitive data), etc.

The security of aggregated data is governed by the information security strategy and plans, and spans physical, logical, and operational domains. The physical domain includes the networks and the directly connected systems. The logical domain includes the ways in which users access and authenticate to system and network resources related to aggregated data. This domain is typically governed by an information security department and by the immediate department where the systems reside. The operational domain, somewhat more fragmented, considers how and where certain mission-related functions are performed, ultimately by the owners and users of aggregated data.

Audit and Monitoring: Monitoring and auditing inspects and examines the degree to which the organization's policies are being implemented and followed. Monitoring activities are the means by which the organization systematically checks its security posture for weaknesses and vulnerabilities, and initiates appropriate responses where necessary. This includes observing system and network events, configurations, and processes under routine operation for suspicious or unauthorized events related to aggregated data security. The practices and technologies supporting monitoring require the expected or normal state of the system and network environment to be known and defined for aggregated data in processing, storage, and transmission. Where monitoring is the more continuous activity integrated into the organization's routine system administration and management, auditing inspects the security safeguards and controls to determine whether they comply with regulatory and legal requirements, policies, and standards.

Vulnerability Management: Vulnerability management determines the state of technical and operational weaknesses in the technical infrastructure where aggregated data resides, and how to appropriately mitigate the weaknesses. Vulnerability assessment is a proactive or preventive monitoring activity where systems and networks are examined for known technical flaws or weaknesses. Results of a vulnerability assessment are analyzed, prioritized, and reported, with actions tracked to completion.

Aggregated data is one form of information and benefits from the same organizational, process, technical, and human security controls that are well known and practiced in information security. Problems and issues unique to aggregated data and its inherent characteristics have been described in Section 3. Risks and impacts to electronic information have been summarized in Section 4 and interpreted for some of the unique challenges that come with owning, using, and serving as custodians for aggregated data. The principles and practices briefly described in Section 5 apply to most types of information and information systems. This paper suggests using such principles and practices, as part of an organization-wide security strategy, to adequately protect aggregated data. By doing so, organizations are more likely to be able to demonstrate that they are exercising due diligence through following commonly accepted good practice.

Appendix A

The principles described in Section 5 are derived from several credible and reputable organizations and the sources listed in Table 1.

Table 1: Sources of Enterprise Security Principles

Organizations	References
American Chemistry Council	[ACC 99, ACC 03]
Business Software Alliance	[BSA 03]
Corporate Governance Task Force	[CGTF 04]
Corporate Information Security Working Group	[CISWG 04a, CISWG 04b]
Information Systems Security Association	[ISSA 04]
Information Technology Governance Institute	[ITGI 01, ITGI 04]
Institute of Internal Auditors	[IIA 01]
International Standards Organization (ISO)	[ISO 00a, ISO 00b]
National Association of Corporate Directors	[NACD 01]
National Institute of Standards and Technology	[NIST 96, NIST 04]
Organisation for Economic Co-operation and Development	[OECD 02]
Software Engineering Institute	[CMMI 03]

[ACC 99] American Chemistry Council. *Responsible Care® Guiding Principles*, 1999. http://www.americanchemistry.com/.

[ACC 03] American Chemistry Council. *Responsible Care® Security Code of Management Practices*, 2003. http://www.americanchemistry.com/.

[BSA 03] Business Software Alliance. “Information Security Governance: Toward a Framework for Action.” October 2003. http://www.bsa.org /resources/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=5841&hitboxdone=yes.

[CGTF 04] Corporate Governance Task Force. “Information Security Governance: A Call to Action.” National Cyber Security Partnership, April 2004. http://www.cyberpartnership.org.

[CISWG 04a] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. “Report of the Best Practices Subgroup.” March 3, 2004. http://reform.house.gov/TIPRC /News/DocumentSingle.aspx?DocumentID=3030.

[CISWG 04b] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. “Report of the Best Practices and Metrics Teams.” November 17, 2004; updated January 10, 2005. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661.

[ISSA 04] Information Systems Security Association. “Generally Accepted Information Security Principles v3.0.” http://www.issa.org/gaisp/gaisp.html (2005).

[ITGI 01] Information Technology Governance Institute. “Information Security Governance: Guidance for Boards of Directors and Executive Management.” Information Systems Audit and Control Foundation, 2001. http://www.itpi.org.

[ITGI 04] Information Technology Governance Institute. “COBIT Security Baseline: An Information Security Survival Kit.” ITGI, 2004. Individual checklists are available at http://www.itgi.org.

[IIA 01]The Institute of Internal Auditors et al. “Information Security Governance: What Directors Need to Know.” IIA, 2001. http://www.theiia.org/iia/index.cfm?doc_id=3061.

[ISO 00a] International Standards Organisation. ISO 9000:2000 *Quality Management Systems – Fundamentals and Vocabulary*; Second Edition 2000-12-15. ISO 9000:2000(E), 2000.

[ISO 05] International Standards Organization. ISO/IEC 17799 / Information Technology - Security Techniques - Code of Practice for Information Security Management / Second edition/. ISO/IEC 17799:2005(E). June 2005.

[NACD 01] National Association of Corporate Directors. “Risk Oversight: Board Lessons from Turbulent Times.” *Director’s Monthly Newsletter*, 27, 1. NACD, January 2003.

[NIST 96] Swanson, Marianne & Guttman, Barbara. “Generally Accepted Principles and Practices for Securing Information Technology Systems” (NIST Special Publication 800-14). National Institute of Standards and Technology, September 1996. http://csrc.nist.gov/publications/nistpubs/.

[NIST 04] Stoneburner, Gary, et al. “Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.” NIST Special Publication 800-27 Rev A, National Institute of Standards and Technology, June 2004. http://csrc.nist.gov/publications/nistpubs/.

[OECD 02] Organisation for Economic Co-Operation and Development. “OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.” OECD, 2002. http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

[CMMI 03] Capability Maturity Model® Integration. Carnegie Mellon University, Software Engineering Institute. http://www.sei.cmu.edu/cmmi/cmmi.html.

References

URLs are valid as of the publication date of this document.

[Allen 05] Allen, Julia. *Governing for Enterprise Security* (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tn023.html.

[Berkley 00] Anonymous. "Data Powers of Ten." University of California at Berkley, 2000. Avaliable at http://www.sims.berkeley.edu/research/projects/how-much-info/datapowers.html. References original work by Roy Williams of the California Institute of Technology in the mid-1990s.

[Braun 04] Braun, Robert & Stahl, Stan. "An Emerging Information Security Minimum Standard of Due Care." Citadel Information Group, Inc., 2004. http://www.citadel-information.com/min-std-due-care.pdf.

[Charette 05] Charette, Robert. Review comments on [Allen 05], May 2005.

[CRS 05] Fischer, Eric. "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options." Order Code RL32777. Congressional Research Service, Library of Congress, February 22, 2005. http://www.thecre.com/pdf/secure/20050404_cyber.pdf.

[Gartner 04] Hallawell, Arabella. "Gartner Global Security and Privacy Best Practices." Gartner Analyst Reports, March 16, 2004. Available at http://www.csoonline.com/analyst/report2332.html.

[Geer 04] Geer, Daniel E. "Why Information Security Matters." Cutter Consortium Business-IT Strategies Vol. 7, No. 3, 2004.

[Mearian 05] Mearian, Lucas. "The 100-Year Archive Dilemma." ComputerWorld, July 25, 2005. Available at http://www.computerworld.com/hardwaretopics/storage/story/0,10801,103382,00.html.

[Orzech 03] Orzech, Dan. "Rapidly Falling Storage Costs Mean Bigger Databases, New Applications." CIO Update – Technology Trends, June 4, 2003. Available at http://www.cioupdate.com/trends/article.php/2217351.

[Webster 05] Merriam-Webster, Inc. *Merriam-Webster Online Dictionary*, 2005. http://www.m-w.com/.