



I Dentity Management: **A CHALLENGE TO BUSINESS COMPETITIVENESS**

INTRODUCTION

The lack of effective Identity Management (IDM) policies is causing some businesses to lose the trust and loyalty of their customers. Robust IDM policies can improve brand image, increase loyalty among consumers, suppliers and employees, and improve the bottom line.

To maximize the return on investment from creating and implementing a comprehensive first-class IDM system, businesses need to consider moving beyond IDM policies solely drafted to comply with regulatory requirements; but rather, adopting IDM policies that recognize customers—not products—as the source of revenue.

Implementing IDM policies that establish and maintain customer trust and loyalty to the benefit of the whole company will require the leadership of CEOs, CFOs, and the like; the implications of failure are too great to be left solely in the hands of IT specialists.

BACKGROUND

As a leader in innovation, the United States has frequently looked to technology to solve many of society's troubles. In the case of IDM, new technologies may indeed offer some increased risk mitigation, but new technologies also will provide the means for the criminal and negligent to undermine business attempts to protect personally identifiable information (PII). Thus far, the search for technical solutions has caused many in the business community to perceive the issue solely as an expense to be relegated to their company's information technology department.

Effective IDM requires a combination of the right technologies and the right management policies to ensure a corporate culture that builds IDM into day-to-day operations. Poor IDM policies may destroy carefully built brand images, dissolve customer trust and loyalty, confound efforts to operate globally, undermine the profitability of the company as a whole, and seriously diminish shareholder value. Finding solutions may be all the more challenging for companies operating in foreign cultures and regulatory environments.

Overcoming the risk created by a poor IDM policy and discerning solutions applicable on a global basis will require America's business executives to take a hands-on approach and lead by example.

DEFINING IDENTITY MANAGEMENT

Although there are generally accepted factors used to describe IDM, there is no single accepted definition. The use of policy-based processes and technological tools to create, manage, and eliminate identities, and allow access to resources—including the delivery of on-demand or personalized services or products—based upon an authenticated identity, may be considered IDM. This definition may work in a textbook, but when it comes to operating a successful business, this definition may lead decision-makers to the erroneous conclusion that IDM is solely a technical issue.

In fact, the goal of creating IDM policies for businesses should probably be establishing and maintaining an environment of trust with its customers (both internal and external).

Consumers, suppliers, and employees are most likely not interested in the processes and tools a company uses to manage personally identifiable information; instead, they are interested in getting an answer to a very simple question, “do I trust this company?”

IDENTITY INCIDENTS INCREASE

Hardly a day passes by without a story of identity mismanagement making the news. There seems to be no limit to the types of businesses and institutions affected, as educational institutions, government agencies, brick-and-mortar retail establishments, financial services companies, online search engines, and many other types of businesses have all suffered adverse publicity for their inability to live up to the trust given them by their customers.

Many of the most publicized incidents are data breaches resulting from computer hacking, the use of malware, or incorrect handling of laptops and portable media. Even if data breaches do not necessarily lead to identity theft, any publicized large-scale breach probably raises identity theft concerns among consumers and may foster feelings of distrust.

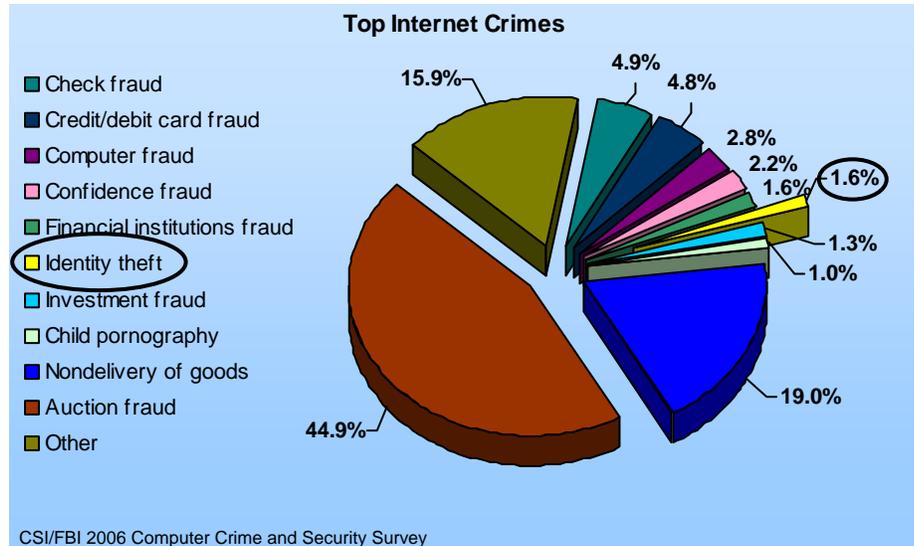
The Ponemon Institute’s figures indicate that the public has increasingly become more concerned about being a victim of identity theft. In January 2005, only 30 percent of respondents were concerned about identity theft; however, by December 2006 that number had risen to 60 percent.

Identity theft, although ranked ninth in the top ten complaints of internet crime, accounted for just 1.6 percent of the total number of complaints received by the Internet Crime Complaint Center (IC3). In 2006, fraud was the number one Internet crime complaint according to IC3. More than 60 percent of complaints received by IC3 (a partnership of the FBI and the National White Collar Crime Center) concerned auction fraud, check fraud, credit card fraud, confidence fraud, or

investment fraud (see “Top Internet Crimes” table). Many of these Internet crimes could be prevented by effective identity management policies and implementation.

It is possible that one of the reasons customers now express such a high level of anxiety about “identity theft” is that they may not distinguish between

identity theft and other categories of internet crime such as fraud.



It is not difficult to see why customers might blur the distinctions between identity theft and fraud. Customers may think that in order for most internet crimes to be committed, someone must:

1. Defeat a company’s authentication scheme;
2. Steal a critical element of their identity; and,
3. Misuse an attribute of their identity to engage in fraud.

Labels, headlines, and rumors aside, available data does support customers’ increased general apprehension about how their identity is stored and managed electronically. The Privacy Rights Clearinghouse reports that public disclosures concerning data breaches in the United States since January 2005 indicate that at least 159,054,253 records containing sensitive personal information were lost or stolen.

THE CHALLENGE

The challenge to business is how to integrate IDM best practices into everyday business operations—not just electronic commerce—realizing that good IDM increases profitability and improves competitiveness.

Consumers, employees, and suppliers all possess a basic expectation that any of their identity-related information will be managed in a way that will, in Hippocratic fashion, first do no harm. If businesses do no more than meet this objective, a perception of trustworthiness results. Nevertheless, as the general public becomes more aware of incidents where the privacy of PII is not maintained, customers may not excuse even a single instance of lost PII without an extraordinary attempt by business to retain their loyalty.

Consumers today are much more aware that competition exists among goods suppliers and/or services providers, in large part due to information available on the Internet. According to Alton Adams, managing partner at Accenture, "Companies need to work harder and harder to maintain loyalty because of the Internet." Losing a customer's trust through unsound IDM policies may cause a customer to explore their alternatives with competitors.

REMAINING COMPETITIVE—MAXIMIZING VALUE

The opportunity exists for any business to differentiate themselves from their competitors through company policies that encourage the integration of superior IDM principles and practices into their operations. Even superior IDM principles may lose their effectiveness if a company's policies only encourage their adoption as an "add on" to a company's operations as opposed to fully integrating IDM principles. One result of gold standard IDM policies is an increase in trust.

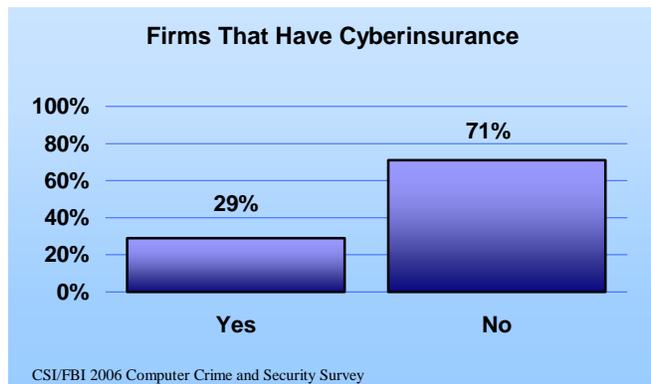
A recent Oakland University study tested several hypotheses among a sample of young adult Internet users and found statistically significant results that indicate:

- Privacy protection does lead to greater customer trust;
- Customer trust leads to customer truthfulness and loyalty; and,
- Trust mediates the relationship linking privacy and customer loyalty.

Perhaps it is just a matter of common sense that **trust breeds loyalty, and loyalty creates economic value**. In a trusted relationship, the buyer saves purchasing time, is more open to ideas, and is more forthcoming about relevant information. The seller gets reduced sales costs, better pricing, and access to important knowledge to improve products or services.

Lower Cyber Insurance Costs

Beyond improving profits from sale of goods and provision of services through increased trust, solid IDM policies bring other tangible and intangible benefits. For example, many companies today find themselves unable to afford insurance against breaches of their IDM systems. Premiums can range from \$5,000 to up to \$60,000 per \$1 million of coverage, depending on the size of a company, the depth of services it offers, and its exposure to risk.



Businesses that have meaningful IDM policies in place may receive 15–20 percent discounts on premiums. It is important to note that according to the Ponemon Institute, the average cost to a company per lost customer record now stands at \$182. Accordingly, businesses should consider cyber insurance, as it could be an important benefit.

GAINING ACCESS TO FOREIGN MARKETS

Implementing top-notch IDM policies may also lead to new international customers, whom previously may have been dissuaded by businesses' apparent lack of compliance with their government's regulations. A number of governments have adopted regulations for aspects of IDM, such as protecting PII, but there appears to be little evidence of commonality across borders.

For example, in 1995, the European Union enacted the "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." This directive, in general, requires the unambiguous consent of a data subject before his or her data can be processed. Globally, Australia, New Zealand, Canada, South Africa, Chile, Argentina, and Japan also have active data privacy laws.

It would seem impossible that even a best-practices approach to IDM could satisfy all the regulating jurisdictions and the requirement regarding the protection of PII, but it is certainly the case that following IDM best practices could allow access to some lucrative foreign markets.

In the case of Europe, the U.S. Department of Commerce developed a "Safe Harbor" framework that allows businesses to self-certify that they provide "adequate" privacy protection, as defined by the Directive (additional information is available at <http://www.export.gov/safeharbor/index.html>). Those U.S. businesses that self-certify to Safe Harbor are not restricted from accessing EU customers' data, ensuring uninterrupted transfers of personal information worth billions from the EU to the United States.

IMPORTANT FOR COMPANIES—SMALL, MEDIUM, AND LARGE

While all companies that create, process, or store identifiable information received from consumers, suppliers, or employees need comprehensive IDM policies, small and medium-sized enterprises (SME) face some different issues from those of multi-national enterprises (MNE). The differences for SMEs primarily involve implementation and monitoring issues. According to *The Eleventh Annual Computer Crime and Security Survey*, businesses with high annual revenue outsource a greater percentage of computer security functions. In addition, companies with more than \$10 million in annual revenue have significantly lower average computer security expenditures per employee (\$126–\$461) than companies with less than \$10 million in annual revenue (\$1,349 per employee). So, one unsurprising difference between SMEs and MNEs is that SMEs will have to spend a greater percentage of their annual revenue to implement an IDM system.

The major differences that SMEs face in creating and implementing IDM come down to affordability, degree of exposure, and ability to absorb the costs resulting from data security breaches.

Multinational enterprises face additional challenges in implementing IDM systems. While operating in multiple regulatory environments, MNEs still need to arrive at comprehensive and consistent IDM policies throughout their operations—and without creating confusion and disagreement among a diverse workforce. MNEs may also find it more difficult to create a culture of security business-wide as customers, employees, and suppliers may have very different concepts of appropriate IDM policies based upon their culture and history. The communication problems inherent in operating any large enterprise may also create difficulties for MNEs that SMEs are less likely to face.

CONCLUSIONS

Identity management is a huge and sometimes confusing topic that must be addressed adequately by U.S. businesses if they wish to remain competitive in the global market. Those businesses that understand that effective IDM policies are a necessary component of creating value for customers will adopt and implement appropriate policy-based processes and technologies, resulting in a competitive advantage over those companies that fail to do so.

If these issues are not addressed, governments will feel pressured to take actions in the form of legislation and regulation that may not be optimal for business and may have the unintended consequence of creating barriers to international business. In addition, despite best efforts, different governments will most likely take differing approaches, meaning that companies will have to comply with numerous different—and costly—requirements.

An opportunity now exists for business executives to take the lead on resolving IDM issues through implementation of comprehensive integrated best practices. Businesses should act swiftly as this opening may not last long in the face of mounting public pressure for legislation.

Looking Forward:

- Should government assume a facilitative responsibility, or play a more direct role for effective IDM policies to flourish?
- What's the best way to promulgate best practices in IDM, especially to SMEs?
- What are the implications for business, as foreign jurisdictions create and re-define regulations and policies related to protecting personal data as an element of identity management?
- What identity management models exist that reflect the IDM interests of consumers, industry, and government?

For more information about this paper—produced by the Office of Technology and Electronic Commerce of the International Trade Administration's Manufacturing and Services unit—contact Scott Mathews at: scott.mathews@mail.doc.gov.

Sources

Gordon, Lawrence A., et.al, *Eleventh Annual CSI/FBI Computer Crime and Security Survey*, (Computer Security Institute; www.GoCSI.com) 2007

Lauer, Tom and Xiaodong Deng, "Building Online Trust Through Privacy Policies," (Oakland University, Rochester MI) 2006

Machal-Fulks, Julie and Robert J. Scott, *Privacy, Network Security and the Law*, (Scott & Scott; Dallas TX) 2007

National Institute of Standards and Technology, Computer Security Division, *2006 Annual Report*, (U.S. Department of Commerce; Washington, DC, 2007)

National White Collar Crime Center and Federal Bureau of Investigation, *Internet Crime Report, January 1, 2006–December 31, 2006*, (Internet Crime Complaint Center; (http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf) 2007

Ponemon, Lawrence E. "Key Privacy Challenges of the New Century Institute" (The Privacy Symposium, Cambridge MA) August 21-24, 2007

Privacy Rights Clearinghouse, www.privacyrights.org/identity.htm

U.S. Department of Commerce, Safe Harbor, www.export.gov/safeharbor

Weill, Peter and Sinan Aral, "Generating Premium Returns on Your IT Investments," *MIT Sloan Management Review* (Massachusetts Institute of Technology, Cambridge, MA) winter 2006