

Identity Theft

How Companies – and Consumers – Can Protect Themselves

Identity theft has become one of the fastest-growing white collar crimes in the world. Just as infectious diseases can today spread faster due to technological developments like affordable jet travel, so too has the growth of identity theft exploded because of the Internet and the ubiquity of powerful computer databases.

By Alan Brill and Troy Allen

This unfortunate expansion has brought identity theft far beyond its origins of petty thieves pilfering wallets and stealing letters from mailboxes. Violent felons and organized crime now engage in high-volume identity thefts to finance a wide variety of illegal activities. No matter who perpetrates it, identity theft is a crime – at least in those countries that have passed actual laws against it – that wreaks its own special brand of havoc. Its victims can spend hundreds of hours and thousands of dollars trying to regain control of sensitive personal information, restore credit ratings, and deflect court judgments or lawsuits.



When one considers that we are all potential targets of identity theft, the economic and social effects of this crime become clear. In fact, identity theft affects approximately 10 million Americans every year. A recent survey estimates that the dollar value of the crime was \$52.6 billion in 2004.

How can consumers protect themselves in a system that was never designed to be highly secure? And how can companies ensure the integrity and security of sensitive customer and employee data? While there are no perfect solutions, every business should take reasonable steps to reduce risk and to know what to do if an incident occurs.

The cold, hard truth is that identity thieves know what they need, and they know where and how to get it. So what is it, exactly, that they are after? It's the electronic and hard-copy files that almost all organizations store on both current and former employees, customers, and consumers. Unfortunately, this data is sometimes far too easy to access because of weaknesses in physical security, corporate policies and procedures, and IT security.

A Multidimensional Approach

From the viewpoint of corporate managers, the issue is twofold. Organizations must safeguard sensitive data, and if security measures fail and a breach occurs, they must respond quickly and effectively.

Because the problem is complex, the solution must be multi-dimensional. Computer security may be very strong, for example, but all the firewalls in the world won't stop temporary employees from using their unrestricted access to copy gigabytes of sensitive data onto an MP3 player that can serve as a hard drive when attached to an unprotected computer.

At Kroll, we've been involved in the various aspects of the identity theft problem for years. We've recognized that the total skill set needed to both defend against the identity theft problem and take action when a breach occurs is very broad,

requiring the knowledge and experience of a number of specialists. This need exists for almost all organizations today. Based on our experience, the following corporate functions need to actively participate in identity theft prevention and incident management:

- Senior management
- Information technology
- Risk management
- Corporate security
- General counsel
- Human resources
- Internal audit

When we look at cases involving significant breaches of sensitive personal information, we see that often the damage could have been mitigated – or completely avoided – through preventive measures. Few, if any, of the victimized organizations truly understood or recognized the total scope of their exposures. Of those that did, fewer still were willing to commit the resources to implement the necessary safeguards.

In other cases, the problem is not with prevention (some incidents are almost impossible to prevent) but instead with an ineffective response to an incident. The very worst reaction is to try and “cover up” an incident or sweep it under the proverbial rug, which only creates additional liability and reputational risk for the organization.

Let’s look at some of the different kinds of incidents, and see how both preventive and post-incident activities require cooperation among an organization’s functions.



Low-Tech Attacks

With all the recent publicity over hacker-related mass identity theft, it is easy to forget that some of the greatest corporate vulnerabilities do not involve high-tech attacks. Consider the following cases:

Theft of back-up files

There have been a number of reported cases of loss of back-up tapes, either in transit to a storage facility or while in the hands of a storage-facility vendor. For example, in one 2004 incident, tapes containing bank records of almost four million customers went missing during the shipping process. Whether the fault was with the company or the shipper, those four million people were placed at risk of identity theft.

Best-practice standards now require that back-up tapes be encrypted, so if the tape is lost, sensitive information will still be protected. But there's more that can be done to protect back-up files and other data in transit. Implementing exceptional security practices within an organization means that shipping or offsite storage must be held to the same high-level security and operational standards to which the organization holds itself.

Involving the risk manager in this issue is important. This professional can help assess the insurance provided by the storage vendor, for example. Corporate counsel should also be involved in assessing the contractual provisions of any vendor agreement. In some cases, corporate security, internal audit specialists, or an independent third party can help by providing an assessment of the vendor's physical and operational security practices. Recently, Kroll had a case in which a client had never checked on the security practices of a vendor. It turned out that security issues at the vendor's site were so serious that the client terminated its relationship with the vendor.

Global outsourcing risks

In a recent case, a British reporter traveled to India and bought confidential personal information on U.K. nationals from a call-center outsourcing firm. As it turned out, Indian law did not clearly establish this to be a crime. In addition, conducting background checks on employees in such organizations was not routine in India.

Before entrusting sensitive or highly proprietary information to an offshore vendor, it is vital to understand both the legal system in the vendor's geography and to verify how the vendor plans to safeguard the data.

Some vendors may have taken the steps needed to become accredited under recognized international standards (such as ISO 17799). In other cases, a company may want to predicate its vendor selection on the results of an on-site review performed by a globally recognized security assessment group. Companies should be mindful of assurances provided by vendors who offer reports by reviewers no more well-known than they are. A company's level of trust in a report can only be as sure as its trust in the firm providing it. In many cases, it is appropriate for the vendor to provide such a report. In other cases, reports are commissioned under the "trust, but verify" concept.

Carelessness and lax standards

Over the past year, several high-profile identity theft cases have made the news:

- A vendor of consumer information failed to check the validity of companies buying the information. It discovered that a small number were scam companies that existed solely to obtain records for potential identity thefts. That company has now instituted far more extensive customer checks.
- A university employee's laptop computer, containing a large volume of student and applicant data, was stolen. The information was not encrypted or otherwise protected.

- Several major corporations reported that they had simply “lost” substantial amounts of data, information that they believed had been safely stored.

None of these cases involves weaknesses in computer security or network security. Rather, each case represents a human failure, such as a lack of attention to basic security and a failure to implement reasonable safeguards.

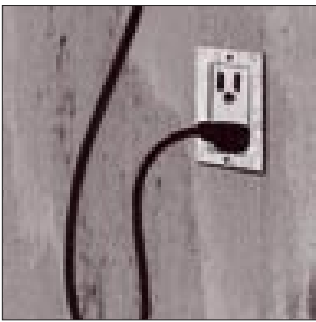
High-Tech Attacks

Of course, some identity theft attacks occur through technical means, such as exploiting weaknesses in computer hardware or software. In these cases, hackers take advantage of problems in operating systems, Internet browsers, firewalls, or internal processing software to gain unauthorized access to confidential data.

Investigation of such incidents shows that these attacks can often be thwarted with the right preventative measures.

Among them:

- Keeping current with security software updates (sometimes called “patches”). An unpatched system is, by definition, operating with known weaknesses, and these weaknesses act as invitations to hackers. But applying patches takes time and resources, and it’s up to senior management to insist that security updates be handled quickly and effectively.
- Knowing where important customer data resides. Every company should engage in data flow mapping, which provides an objective basis for company managers to track information and understand who will have access to data while it stays within the company’s purview. The point is to create a “trail” so that data doesn’t just proliferate randomly in different electronic nooks and corners of the company, where it can be accessed or stumbled upon by an opportunistic employee, contractor, freelancer, or hacker.



- Collecting evidence when an incident occurs. Failure to collect evidence in a forensically sound manner can make it impossible to pursue criminal charges or to seek civil restitution. Having qualified computer forensic resources, either in-house or readily on call, should be a part of every company's plan.
- Recognizing the risks of wireless data transmission. We have seen many instances in which companies did not properly secure wireless networks. During one investigation, Kroll discovered that company employees had installed their own wireless routers to enable laptop connections, with no need for additional network cables. Not surprisingly, the network was not properly protected, and when we measured the signal transmission distances, it was apparent that the unauthorized network could be accessed from outside the company's building. Regular testing to ensure that no one is running a rogue network, and that authorized wireless networks are properly protected, is vital.

Avoiding Predictable Problems

Both high-tech and low-tech identity theft attacks hinge on various corporate vulnerabilities that facilitate the pilfering of sensitive customer data.

Data that shouldn't be there in the first place

When we investigate identity theft incidents, we often find that much of the stolen data should never have been obtained and/or retained. As data storage has become less and less costly, many companies simply don't bother to clear information out of their systems. Companies must use the principle of data minimization, which states that:

- A company should retain only that data that can be linked to a specific requirement of a necessary business process. Collecting sensitive data that isn't needed represents 100% risk and 0% payback.

- Eliminate data that's no longer needed. Once a customer transaction has cleared and the period in which the customer can get a refund is over, why keep the credit card number on file (unless, of course, the customer asks you to keep it on file)? Data that was once needed, but that is no longer required, represents another high risk, with no compensating business need.
- Reduce the number of places data is stored. If there is not a legitimate business need, companies should limit the number of electronic and hard-copy locations in which sensitive personal data is maintained.
- Re-evaluate data minimization on at least an annual basis. In the event of a merger, make sure any acquired systems go through a data minimization analysis. This is an area where both internal audit and specialized external resources may be very useful.



Rigorous enforcement of corporate policies and procedures is critical to this principle's success. Many breaches of data occur when employees store data on laptops and local drives, or take home hard-copy files, exposing them to potential identity thieves.

Employees who should never have been hired

When companies give employees access to sensitive customer data, they are entrusting them with an asset that, if mishandled, can literally put the company out of business. With that level of risk, it constantly amazes Kroll investigators that companies neglect to do thorough background checks on those who can access such data. In post-incident investigations, we've seen cases where the people involved would never have been hired if a competent background check was done.

Even when hiring professionals for key management posts, the candidate's job history and educational credentials should be verified. While many organizations try to accomplish this on a "do-it-yourself" basis, this is an area in which – due to the

legal and regulatory pitfalls of trying to perform background checks – even very large companies have concluded that engaging experts is the most cost-effective solution.

Temporary and contract personnel with unknown motives

Temporary and contract personnel need to be held to the same high standards as any full-time employee. Numerous incidents have been traced back to “temps” and contract workers. We’ve found that security in regard to these workers often falls through the cracks. HR departments typically perform background checks only on employees.



We’ve also seen that most companies lack processes to brief temps and contractors on security rules, and few use confidentiality agreements with these workers. This doesn’t make sense. Why would a company require employees to undergo background checks and sign confidentiality agreements but allow a non-employee to access that same material with no background check or confidentiality agreement in place? This is an area in which the combined skills of corporate counsel, human resources, and internal auditors can play an important role.

If an Incident Does Occur

We wish we could say that a comprehensive program of high-tech and low-tech security measures could provide 100% protection. But there are always things that can go wrong in any security setting, and that’s true for identity theft, as well.

Perhaps a hacker exploits a previously unknown and unreported security flaw in a company’s software. Or a trusted employee, contractor, or vendor turns out to be not so trustworthy after all.

One thing is clear: Any company that collects or stores sensitive data must devise a carefully thought out plan for handling identity theft incidents. These plans are particularly important in light of emerging legislation that mandates rapid disclosure of incidents to actual and potential victims. Criminal penalties

for failure to make prompt disclosure of incidents are included in some versions of this legislation.

The response plan

Understanding a particular incident may require IT and computer forensics professionals, of course, but also representatives from HR, corporate security, and internal audit.

The response plan must enable the rapid analysis of what happened. It must pinpoint the data involved to facilitate the subsequent incident reporting. Evidence must be collected properly, not only to support prosecution of wrongdoers, but to provide the basis for defending the company against lawsuits that may arise from the incident. Plans must also be updated constantly to meet changing legal and regulatory requirements.

At Kroll, we've seen how the actual act of notification of victims can completely overwhelm a company. After all, what organization can easily print, stuff, stamp and mail 250,000 notifications within a very short time frame? For this reason, it's wise to have an outsourced solution in place, with costs anticipated and contracts signed.

The plan must also take into account potential media and consumer backlash. A spokesperson should be identified who can be the designated point of contact for all inquiries and communicate what the company is doing about the incident.

As part of any response plan, companies must also determine how they are going to help the victims. This help can range from credit monitoring of limited duration to full-scale identity-restoration services. Many alternatives are available from outsourcing vendors.

Most importantly, the response plan needs to be tested before an incident occurs. Waiting for an actual incident may be too late. If there are problems with the plan – something completely overlooked, or an element that just won't work in practice – it's better to realize so before the incident becomes headline news. Just as the terrible events of September 11, 2001 taught companies to test their business continuity plans before a disaster occurs, the continuing string of identity theft incidents should be the warning to corporate executives to develop and test identity theft incident plans.

Conclusion

Identity theft has become a problem that nobody can afford to ignore. While there are no absolute solutions, there are many well-documented methods to reduce risk and handle incidents effectively.

For every company, the risks will be slightly different. But with preparation, planning, and the recognition that a wide range of skill sets are needed to thwart this crime, any company can meet the challenge.

Alan Brill is senior managing director, Technology Services, for Kroll Ontrack

Troy Allen is senior vice president, Fraud Solutions, for Kroll Background America

