

Security Unleashed

A hand holding a key over a lock on a door. The background is a solid blue color. The key is black and the hand is holding it from the right side. The lock is on the left side of the door. The text "Security Unleashed" is written in white, sans-serif font across the top half of the image.

There are ways to protect data from prying eyes and keep your business safe. Here are some sleuthing technologies that are bellwethers for 2007.

When it comes to security, the conventional wisdom goes something like this:

If it fails, you don't just lose data or merchandise, but often your customers, revenues, and even your hard-earned reputation and trust. If it succeeds, you've spent a lot of money to maintain the status quo. Security, in short, is a necessary evil. It's a defensive measure, not a tool for growth. But here's the problem with the conventional wisdom: It's completely wrong.

By changing the way they think about security, organizations—whether businesses or government entities—can reap all sorts of new benefits. They can keep their systems, products, and people secure, and at the same time they can find and leverage new opportunities and boost their efficiency. They can discover and eliminate duplicative processes and unnecessary costs. By providing better visibility into the business and its customers, security can reveal promising areas for growth even as it pinpoints would-be problems. Companies that shake off the antiquated image of security can discover a new catalyst for success—and a competitive advantage.

A bank, for example, may have numerous databases scattered throughout its enterprise. Each of these is a target for a hacker, and when a breach occurs, it can take days to figure out which database has been compromised. But by using new technology tools that link systems more holistically into a common framework, the bank not only can enhance security, it can solve problems more quickly. The institution also gains another big benefit: With this type of integrated system, all the parts of the bank now have access to the same real-time information. A deeper, more nuanced view of the customer is possible. The bank can more accurately predict things, like which customers are ripe for a car loan or home refinance.

Implemented wisely, security not only becomes an offensive weapon, but it frees up valuable resources—namely, the top decision-makers who guide an organization's strategy and innovation. "Executives spend too much time worrying about security-related issues, when they should be focused on running their business," says Michael Gibbons, vice president and general manager, enterprise security for Unisys, a global technology services and solutions company.

Looking for Red Flags

Of course, it's hard to blame executives for worrying about security. According to Unisys, IT security vulnerabilities have increased substantially in just the past five years. Where many of these executives go wrong is in

how they define security. It's not just about locking down systems; it's about considering how security pervades an entire enterprise. "Security is about people and processes, too," says Gibbons. "And that means that there are an awful lot of things organizations have to think about, such as building the right controls into their applications, and training employees so they can spot trouble before it happens. It means understanding your risks and how you are managing them."

Implementing this kind of proactive security is a challenging task, however. Clearly, the technology to



get the job done exists. All sorts of tools—from handheld scanners that can track goods in transit, to fingerprint readers that allow only authorized staff into sensitive areas, to sensors that sound the alarm when a hard disk has been tampered with—are readily available, offering better, quicker knowledge about your people, products, and equipment. But tools alone aren't enough. The hard part is striking the right balance between protecting your assets and maintaining your agility.

Unleashing the true power of security means asking the right questions and considering the right factors. What threats do you face? What is the culture of your business? What is the regulatory environment like? What are your competitors and partners doing? Companies don't have to do all the legwork themselves. By partnering with seasoned IT security and business operations experts, organizations can better understand their processes and risks, and what they need to do to implement a system that slams the door on disaster but keeps it open to opportunity. "We'll come in and build a plan with an organization," says Gibbons. "We'll look at how they are managing risk, and we'll look at their people and processes, as well as their technology, to provide a blueprint for decreasing their risks and increasing their efficiencies."

Security doesn't have to be a cost center; it can be a way to boost productivity even as you strengthen your defenses. Already, savvy organizations around the world are finding that they can have the best of both worlds.

By changing the way they think about security, organizations—whether businesses or government entities—can reap all sorts of new benefits.

Fighting Identity Fraud

One of the biggest areas for concern these days—for businesses, governments, and consumers alike—is identity fraud. When Mr. Smith is in fact Mr. Jones, the consequences can be grim. Businesses now lose \$50 billion a year to identity fraud, according to Unisys and other sources.

Often, consumers find themselves having to contact banks and credit-reporting agencies only after the damage has been done. Law enforcement agencies need to worry about everything from fraud to terrorism. Robust and secure identity management is no longer a luxury, but a necessity.

Fortunately, cutting-edge tools can provide businesses with the top-flight security today's world requires. New technologies enable dynamic, rules-based fraud models that can adapt, in real time, to constantly changing security threats. Already, Unisys has helped a number of banks harness the power of these analytics in a virtual data warehouse that leverages existing infrastructure.

By providing a common architecture for security monitoring, Unisys is able to integrate risk-prevention units and allow synergies among multiple product channels and functions (e.g., online banking transactions, branch operations, anti-money-laundering compliance). For example, one fraud model can generate an alert—or prevent a transaction outright—when it sees an online bill payment above a threshold amount that is coming from an Internet location in a suspicious country and going to a payee account with a suspicious address.

Even businesses that have not experienced a data breach need to act. "Phishing" attacks—where fraudsters are able to get account usernames and passwords not by hacking into corporate servers but by sending cleverly disguised e-mails that lead

consumers to divulge the information—are a growing concern. Increasingly, consumers are demanding that businesses take steps to prevent phishing and other methods of stealing personal data.

When businesses do spring into action, they're discovering one essential ingredient to fight increasingly sophisticated cyberthreats: visibility across the entire enterprise. For example, in monitoring

The Trusted Enterprise

Given enough time and money, companies can develop the best processes, buy the most advanced equipment, and recruit the most talented employees. However, earning the "trust" of key stakeholders—from partners to customers to employees—is an intangible asset that is extremely difficult to achieve and even harder to maintain.

Surprisingly, despite its importance to the bottom line, businesses often don't focus on issues related to trust until a breach occurs that threatens to destroy the relationships between an organization and its stakeholders. If the breach is significant enough, rapid erosion of trust can occur, resulting in immediate and irrevocable damage to key business drivers, such as sales, market share, and stock price, among others.

"If your organization can't earn the trust of its constituents or it loses it based on a material event, it is likely to result in significant damage to the company's bottom line," says Larry Ponemon, chairman and founder of Ponemon Institute, a research organization that tracks trust in privacy and information-security practices. "Therefore, if we can understand the factors that either contribute to or decrease trust, we can create a blueprint that organizations can use to remedy their deficiencies."

To determine what characteristics enhance and erode trust, and how they impact different types of organizations and the industries they operate in, Unisys and the Ponemon Institute partnered to create the Trusted Enterprise Index, an international survey that polled senior-level business leaders from a wide range of industries about the importance, impact, and influence of trust in the private and public sectors.

The results of the research revealed several surprises. "We expected to see reciprocity; that if trust increases when you have a certain trait, it decreases when that trait is absent," added Ponemon. "But we found that's not always true. Unethical behavior, for example, erodes trust fast, but ethical behavior doesn't do much to build it. People just assume an organization is ethical."

In fact, the survey identified 31 characteristics of trust, broken down into categories that included innovation, dependability, and economic prudence, and then asked respondents how much each factor built trust when it was present, and how much each factor eroded it when it was missing.

For example, respondents indicated that customer satisfaction, leadership, prudent fiscal management, quality, and customer respect were all characteristics that helped an organization build trust when it was

present, while unethical business practices, customer dissatisfaction, lack of respect for employees and customers, and poor leadership were the most likely factors to erode trust if present in the organization.

Along these lines, the research found a clear disconnect between the views of business and technology leaders on the factors that build and erode trust. IT leaders placed a much stronger emphasis on protecting privacy and IT security, while business leaders focused more on traditional financial metrics.

Perhaps most alarming, the study demonstrated the overall lack of preparedness among business leaders to monitor and protect the trust of their companies. Despite an overall concern about trust and the recognition that it is vital to the success of a corporation, 36% of the respondents admitted that their organizations have no one proactively managing the trust of the company—unlike the way they monitor other key disciplines, such as finance, human resources, and communications.

And while many companies are flying blind when it comes to monitoring trust indicators, more than 70% believe the responsibility should fall on the board of directors or the CEO to ensure that the corporation is acting in a trustworthy manner, and is perceived as such among customers, employees, and investors.

security, banks have traditionally searched for potential attacks in isolated systems that don't communicate. That's inefficient—and often dangerously ineffective. Instead, banks need what's known as a fraud detection ecosystem, such as the solution Unisys is helping to implement for Banorte in Mexico, and other banks around the world. By enabling banks to identify and respond to suspicious activity more quickly, these new systems have proven themselves a far better way to contain and deter fraud attacks. Indeed, this holistic approach allows financial institutions to realize key benefits of secure business operations through increased operational efficiency and more intelligent risk monitoring.

Indeed, if consumers don't see those steps implemented, they are likely to take their business elsewhere. According to the Unisys 2005 Identity Fraud

Global Consumer Report, 66% of bank customers worldwide worry about identity fraud and the safety of their bank and credit card accounts, and 45% are willing to switch banks for better protections against identity theft. What's more, the study, which explored how consumers around the world viewed the growing problem of identity fraud, revealed a significant rise in the willingness of Americans in particular to pay additional bank fees for greater security protection. Nearly 40% of U.S. customers are at least somewhat willing to pay fees for more protection, compared to 27% in a similar U.S. survey conducted by Unisys in 2004. Even a larger number of Americans—50%—would consider switching banks for more protection, compared to 45% last year.

The statistics reveal another crucial point: Banks and other businesses need to change their view of

NOT A SUIT
OF ARMOR.
A RED CAPE.

NOT CAMOUFLAGE.
A NEON SIGN.

Success doesn't come to those who hide. It comes to those who confidently assert their presence in the marketplace and refuse to let fear paralyze their ambition. Unisys Solutions for Secure Business Operations enable you to be more innovative, more competitive, and as bold as you want to be. Come out, come out, wherever you are.

Security unleashed. **UNISYS**
Secure Business Operations. imagine it. done.

www.securityunleashed.com

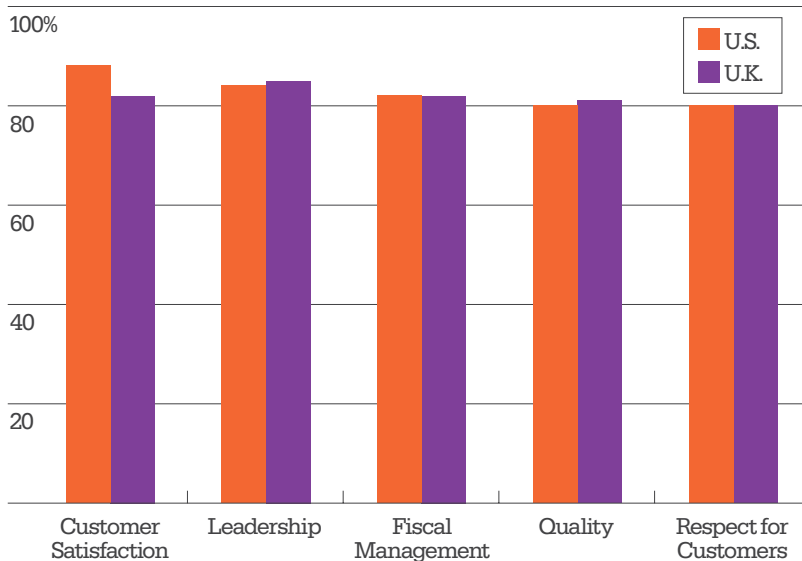
© 2006 Unisys Corporation. Unisys is a registered trademark of Unisys Corporation.

Security unleashed. **UNISYS**
Secure Business Operations. imagine it. done.

www.securityunleashed.com

© 2006 Unisys Corporation. Unisys is a registered trademark of Unisys Corporation.

Building a Valued Brand



Source: The Ponemon Institute and Unisys

How Do Organizations Build/Erode Trust? (U.S. and U.K.)

The top five attributes for building trust across an organization are:

- Customer satisfaction
- Leadership
- Prudent fiscal management
- Quality
- Customer respect

These ranked higher than market capitalization, market share, etc.

The top five attributes that erode trust across an organization are:

- Unethical business practices
- Customer dissatisfaction
- Lack of respect for employees
- Lack of respect for customers
- Poor leadership

security. They should stop thinking of security mainly in terms of firewalls, authentication, and checkmarks on regulatory compliance, but instead as a competitive advantage that customers want and need if they are going to feel good about the institutions they interact with on a regular basis. When customers feel secure, they trust a company more.

Given the importance of customer trust, it has become essential to know which characteristics enhance and erode it, and the impact these attributes have on customer views on security and other issues. This month, Unisys will launch its Trusted Enterprise Index, an ongoing international research project measuring the importance, impact, and influence of trust, privacy, and security in the business and government sectors. (See sidebar.) The index, which surveyed senior executives in both business and technology positions from a wide range of industries, precedes a broad, multi-year global research initiative that will serve as a comprehensive tool for companies and governments to redefine security and business processes.

The Unisys Trusted Enterprise Index, which will initially focus on the United States and Britain (expanding to other markets throughout 2007), builds on the success of the Unisys Security Index in Asia Pacific, introduced earlier this year. The project, like other initiatives at Unisys, is a way of providing companies and governments with the comprehensive tools they need. For example, the index will offer valuable insight

on the challenges companies face in protecting customer privacy while developing robust customer relationship management systems and maintaining strong IT security.

But striking this balance—implementing security so that it meets the needs of both the business and the customer—means that executives on the business side and their counterparts on the technology side have to be in sync. They must understand the technical requirements of their business, as well as the needs and desires of their customers. Then they have to figure out how to serve both entities on a consistent and dependable basis. This task is not as difficult as it sounds. As the Unisys identity fraud research showed, a significant percentage of Americans are willing to pay fees for increased security protection—in fact, more in 2005 than 2004. This and other consumer trends are exactly what financial institutions should be looking at when evaluating security issues.

It's not just Americans who are concerned about security, or willing to accept more responsibility for insuring it by paying those higher fees. The Unisys Asia Pacific Security Index saw an overall rise in consumer fears about security (not just financial security but also national, personal, and Internet security) from just the first to second quarter of the year. (At press time, analysis was underway on third quarter results). Unisys also found that 98% of Australians are willing to use extra security features to protect themselves from threats including identity fraud and misuse of personal information.

The good news: The technology to combat identity fraud and other security concerns has come a long way. Banks and other businesses are working with new tools and learning from the success that governments and other organizations have had with biometrics. Around the world, biometrics—which verifies identity through a person’s unique physiological characteristics, including fingerprints, iris patterns, or voice analysis—are a particularly hot area and a technology that enjoys broad public support.

Another global Unisys study on identity management, conducted in March, found that 71% of respondents in North America held a positive view of biometrics for use in identity management, mirroring similarly high consumer acceptance in other markets around the world. While consumers favor fingerprint and voice recognition technology overall, preferences can change dramatically from one locale to another, and global companies that want to be smart about security need a strong understanding of local considerations. For example, Unisys found that 69% of Australians have a favorable view of iris scans, whereas just over 10% of North Americans do.

The technology is not only convenient, it’s also efficient. Security checks can be processed more quickly through automation. For instance, computers match a person’s biometric attributes with data stored on a central database. Privacy is enhanced, as well. “I’ll carry a smart card with personal information, but the card won’t unlock unless I pass biometrics,” says Gibbons. “So a third party can’t gain access to my data unless I go along with it.”

Biometrics-based identity management has already been put into practice on a large scale in many parts of the world. In Malaysia, for example, nearly 20 million citizens now carry a multipurpose smart card called MyKad that consolidates their driver’s license, banking card, and health services card (complete with confidential information on medical history, allergies, and medications). It can also be used to pay for parking, tolls, goods, and public transportation, and to pass through immigration checkpoints. “We wanted one card that could perform multiple government and private-sector applications, while ensuring the security of the information on the card,” says Datuk Azizan Ayob, former director general of Malaysia’s National Registration Department.

Working with Unisys, the Malaysian government was

Bridging the Gap

A Unisys survey reveals how U.S. companies are managing security and trust issues.



Source: The Ponemon Institute and Unisys

able to link the data on the card to the cardholder’s biometrics—including thumbprint and digital photograph—to ensure that the person presenting the card is the same person whose data is embedded in the card. “This helps us prevent forgery and misuse of data,” says Ayob. Because verification is automated, time-consuming manual checks are no longer necessary. That results in quicker access to key services, like health care, and shorter processing times for everything from bank loans to immigration control.

Tracking the Populace

Biometrics and other security technologies don’t just keep data safe—but people, too. Handheld gamma-ray scanners can check shipping containers arriving in the nation’s ports, ensuring against false walls, contraband, and radiological de-

vices. Fingerprint readers guard against unauthorized access to power plants and other potential terrorist targets.

When enhanced with biometrics, even something as low-tech as a passport becomes a powerful security device. In Australia, e-Passports have an embedded microchip containing a digital photograph to verify the holder’s identity. When broken down into bits and bytes, the photograph becomes a unique set of patterns which sophisticated software can match to the face of the person presenting the passport at an airport. The Australian project successfully demonstrated that facial recognition was a viable technology to tie passport holders to their documentation. Expect to see more countries adopt similar systems: As of October, all visitors to the U.S. from visa-exempt countries (like Australia) are required to present e-Passports containing an integrated microchip capable of storing biometric information.

The projects in Malaysia and Australia—as well as those now taking shape in other countries and companies around the world—show that security can improve processes even as it safeguards them. For governments, it means that borders can be secured without hindering commerce or creating long waits at immigration checkpoints. For consumers, it means better customer service and enhanced protection of vital financial and personal information. For businesses, it means fewer worries about potential risks, and more focus on innovation and growth. ●