Looking Forward: The Challenge of the Decade —Cyber Security

New types of challenges confront technology users. These challenges call for new and effective technologies to identify, authenticate, and protect people, assets and information.

Authored by Ann Grackin

Introduction

Cybercrime today is part of the underworld, as well as part of our public shame. As if to rub in our faces the obvious, the people who hacked Sony Pictures sneeringly told Sony that their decision to withdraw the film from release was a "wise" decision. "We ensure the purity of your data as long as you make no more trouble," the hackers went on to say.

In this report we will discuss the issues in authenticity and identity, build the back story and then discuss solutions and the future of solutions for Identity Management.

Cover Photo Art: © Tashatuvango | Dreamstime.com

Building The Story of Solutions….

The Challenge of the Decade: Securing Systems, Things and People

Cyber Ransom—Hand over the Money and *We Won't Hurt Your Kid*

Okay, Mr. Corporate America, we have your 10-year-old daughter. Hand over your credit card data, your new product designs, your customer lists. No, we won't let her go, but we promise to be 'pure.' I guess the word *creepy* comes to my mind. Terror, maybe, comes to others. A business decision to others. "We have not caved," says Sony, but the message was clear. Not only had Sony servers been hacked, data erased and other information damaged, but there was greater brand and financial damage.[1]

A business decision. Yes. Somewhere along the way, corporations did make decisions on investments. Our research for the Business Priorities 2014 survey regarding priorities and spend for the year showed that cyber and security investments were pretty low on the list.[2] Obviously, last year cyber security did not make the cut. Too bad, because according to FBI Director James Comey, "There are two kinds of big companies in the United States. There are those who've been hacked and those who don't know they've been hacked." Coming from the US's top law enforcement officer, that is a scary thought. And according to Michael Lynton, Sony Entertainment CEO, the FBI said that Sony's cyber security technology was in sync with 90% of the rest of corporate America.

Data collected by Paolo Passeri[3] (Figure 1) shows the types of motivation behind hacks. A politician's reputation is surely low on the list of reasons, but it points to the damage a hacker can do.

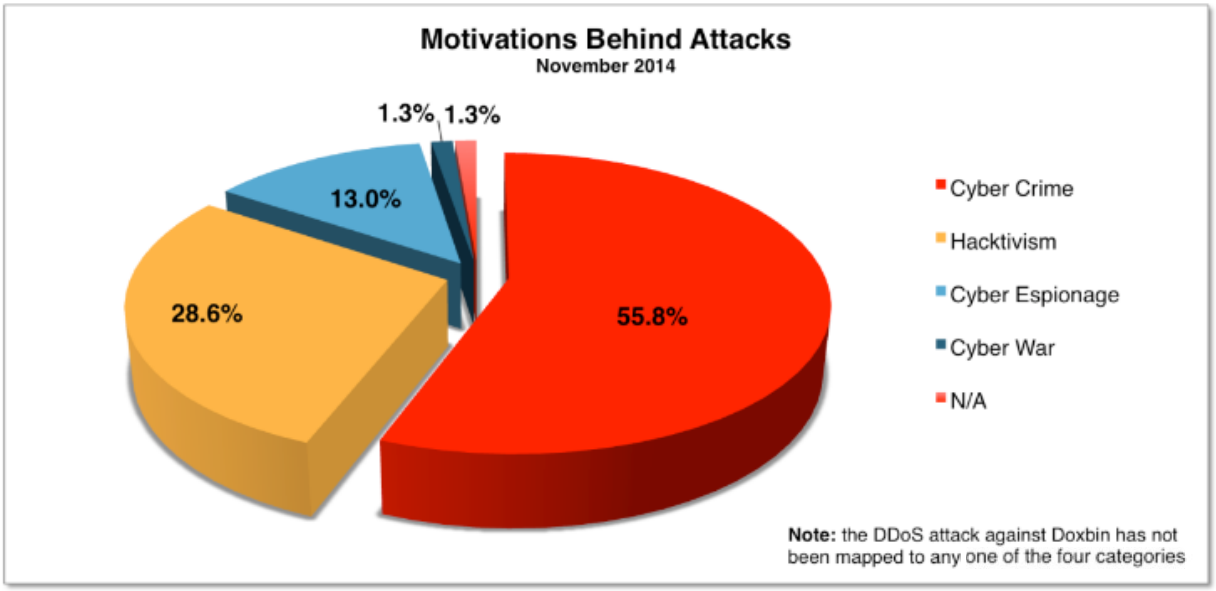

Figure 1: Motivation for Hackers

[1] "We have not caved. We have not given in. We have persevered, and we have not backed down," said CEO of Entertainment, Michael Lynton. "We have always had every desire to have the American public see this movie." Lynton said the studio has contacted video-on-demand and e-commerce sites about distributing "The Interview" online, but no major company has been willing to distribute the film.

[2] You can change that perspective for 2015 by participating in the Business Priorities 2015 Survey.

[3] Paolo is an IT consultant working on cyber security. You can see more hacking statistics on his site or follow him on twitter.

I remember back in 2004ish when my computer was hacked and I called the FBI. I felt violated and vulnerable, as did another 40 million Americans who also were infected by that virus. It changed my perspective. Not long after, the financial company that housed the retirement/401k information for a company I once worked for informed employees that a laptop with all the current, ex- and retired employee data 'went missing' (400,000 employees). Those were the early days.

Famous cases such as Albert Gonzales,[4] who was behind the hacking of TJX, Barnes and Noble, and others, and Max Butler's[5] bank and credit card hacks, seem like child's play today—but those were not victimless crimes, as the hackers claimed. Butler's ring had the death of one ring member, and millions of consumers spending their lives going through all their paperwork (just think of that) forever onward to make sure their finances remained intact, or petitioning to recover stolen funds.

Last year, according to various sources, there were 47K cyber-attacks on companies. Home Depot, PF Chang, Target, eBay, and Apple were on my short list. I am sure you had a similar one. Retailers make the press since their attacks affect so many people (consumers) and they have to report intrusions to the public (we list many of these at the end of this article). In fact, all businesses of all sizes (as we wrote about earlier in the year in Managing Cyber Risks) are targets. And it seems that our financial data also is not safe, since banks are vulnerable, too.[6]

We also know that our nation's competitiveness has been severely impacted by the theft, allegedly by Chinese hackers,[7] of our trade and design secrets.[8] This is sad, since the US is a very open business society in which most of our ideas are shared or at least legally traded with our partners—except the Coke formula, of course.

Securing the Supply Chain—Counterfeits and Illicit Traffic

Tainting, counterfeiting and outright theft is also a 'growth industry.' Customs and law enforcement are proud of their increased rate of catching criminals. And yes, they should be. They are learning the criminals' tricks and are able to catch a percentage of them. But according to the International AntiCounterfeiting Coalition (IACC), US Customs seized $1.7B in counterfeit goods at the border in 2013. According to various sources, that is about 1% to 2% of the total value of counterfeit goods. Worldwide, the stats are about $650B a year of counterfeits. And since counterfeiters also operate within the

[4] Read about Gonzales: Privacy Law Leadership in Cyber Legislation. More on Gonzales, hacking crimes and ring in Wikipedia.

[5] You can view this story on CNBC's American Greed.

[6] **J.P. Morgan Chase:** An attack in June 2014 was not noticed until August of the same year. The contact information for 76 million households and 7 million small businesses was compromised. The hackers may have originated in Russia and may have ties to the Russian government.

[7] Five Chinese hackers indicted. Five Chinese nationals were indicted for computer hacking and economic espionage of U.S. companies between 2006 and 2014. The targeted companies included Westinghouse Electric (energy and utilities), U.S. subsidiaries of SolarWorld AG (industrial), United States Steel (industrial), Allegheny Technologies (technology), United Steel Workers Union (services), Alcoa (industrial), and U.S. Transportation Command contractors (transportation)**.** A Senate report revealed that networks of the U.S. Transportation Command's contractors were successfully breached 50 times between June 2012 and May 2013. At least 20 of the breaches were attributed to attacks originating from China.

[8] **Defense Industries:** Su Bin, a 49-year-old Chinese national, was indicted for hacking defense companies such as Boeing. Between 2009 and 2013, Bin reportedly worked with two other hackers in an attempt to steal manufacturing plans for defense programs, such as the F-35 and F-22 fighter jets.

borders (although internationals are the major sources), many of these criminals operate in plain sight, seemingly with only death and injury as motivation for law enforcement or society to act.

Tainted and counterfeit food and drugs[9] are the biggest concerns due to illness and potential death.[10] "At present, out of the 191 WHO member states, only about 20% are known to have well-developed drug regulation."[11] Not much cover for the industry. Unless enterprises act themselves, or in collaboration with their industry, risk from counterfeiters will continue.

Your Digital Self at Risk

I am who I am, so the song goes. But spammers, hackers and identity thieves seem to think otherwise. The offensive emails I get from 'myself' and other acquaintances whose email accounts have been hacked, attempt to sell me products that a few years back we would have blushed to even think about. Now those products are common knowledge to 7-year-olds who are using their computer for homework and social networking with their friends and relatives.

However, today, you *have* to have a digital self. Even as threats go online, so does everything else. Most business is conducted online—business, government, and personal—so targets and opportunities for hacking will only grow. Having the credentials to conduct and transact business is essential. Effective and yet easy-to-use methods need to be found to protect us and our online identity. Ah, credentials: *Who are you?*

Securing the Data

Today, your company's official communications and transactions are at risk: trade secrets, customer lists and so on. Securing that data and managing the gateway in and out of the company is vital. In talking to the lines of business, many feel that it's IT's job. Way back in my IT manager days, in order to pass 'the audit,' we created some security policies and tried to educate the users about the need for things like passwords, logging out at night, and simple practices that would go a long way in keeping things secure. Tagged as nerds and a pain by the users, our recommendations went unheeded. Today, IT has an arsenal of tools with which to secure the corporation, so things are a bit better. But users still may do some 'off-road driving' from their personal accounts, putting corporate information at risk. However, in the main, corporations can take action and implement techniques to protect themselves. That is if they will just….. *implement them*.

Identity and Authentication: the Gateway to All Things….

In a broader sense, identity is the gateway to it all: the physical and digital worlds—databases, facilities, and finances. How do you know who this company is? Who is this person? Can they be identified? Verified?

---

[9] According to WHO, there are about $200B worth of counterfeits.

[10] According to WHO, counterfeit drugs include:

- Products without active ingredients, 32.1%;
- Products with incorrect quantities of active ingredients, 20.2%;
- Products with wrong ingredients, 21.4%;
- Products with correct quantities of active ingredients but with fake packaging, 15.6%;
- Copies of an original product, 1%; and
- Products with high levels of impurities and contaminants, 8.5%.

[11] The US's Food Safety Modernization Act, due to take effect in 2015, should help pave the way for safer products.

Do they have authority? Most access is based on known people, accounts,[12] and sources.

Authentication goes hand in hand with identification. Does the person have authority to make, touch, handle, label, and so on? What is this item/product? Is it genuine?

What do these terms really mean?

One may define *identity* as the distinctive characteristic belonging to any given individual[13] or group.

To Identify is a bit trickier. It is a label associated with the person or group. You are American; you work for a particular company, live in a certain place. But identifying has to define not just shared traits but individual ones. You are male or you are 24601.[14] These are data about you, but are insufficient to authenticate that it is actually you. More methods are needed. Both digital and physical techniques may be required depending on the use case.

To authenticate means to prove that something is real, true, or genuine.[15] An authority is needed to conduct the process of authenticating. Zoltan Karpathy is the authority in My Fair Lady, for example, with the qualifications to validate that Eliza Doolittle is the genuine article; whereas at a building entrance, a security guard may know you and have the authority to grant you access.

But of course, today, the interconnected world is much larger. Collaboration and communication increasingly must cross enterprise boundaries, and that makes the authentication mission exponentially harder. Each person, thing, user account, and so on, needs some kind of authentication for access to a 'system' and needs to be recognized across systems and organizations. Again, we need several techniques to complete the job—melding digital and physical data with various techniques and algorithms to make sure *you are who you say you are.* In addition, we need solutions that keep track of the interactions, traffic and so on and a neutral gatekeeper, auditor and controller.

Our best and most common example of how this works is the international credit card system: Visa and AMEX cards. ("Recognized the world over" is their advertisement.) Customers should feel secure that the system identifies, authorizes, and protects them and their data. They should also be able to be confident that the entity they are interacting with will be secure and that all will go well. The system identifies the shopper, identifies the merchant and then authorizes the transaction. There are multiple identity activities that occur before a transaction occurs. (This industry, of course, has a lot of issues. We just use this as an example of how systems work across people, processes, and organizations.)

Identity Management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controls their access to system resources by associating individuals with user rights and restrictions within the entity with whom they are engaging. Techniques both physical and digital need to be implemented to define and secure identity. Ultimately, authenticating and identifying go hand in hand, and no single approach has worked so far to really ensure the trust. Hence, a set of technologies needs to work in concert to achieve the goal. In the last few years, there has been a profusion of broader solutions and services to support Identity Management.[16]

---

[12] Authentication of an individual's identity to confirm who they are and to control access to assets, accounts, locations and so on based on that individual's assigned permissions and privileges

[13] Wikipedia

[14] Jean Val Jean's prison identification

[15] Webster's Dictionary

[16] The goal here is not to define and catalogue all the security and anti-virus systems for IT Managers. Our audience is supply chain and product people; thus, the goal here is to address the problem from that perspective. Line of business users such as

Solutions are Needed

Since identity is both a physical and digital challenge, technologies that address both are needed: for example, biometric data—your fingerprint or retinal scan in combination with a password. Or a pin number in association with a pin chip. In addition, the underlying architectures themselves have to be able to securely utilize the systems of identity. Obviously, this underlying infrastructure has had a headache of late with the rash of hacking.

Photo Art: © Vukas | Dreamstime.com

Open and Closed Systems and the Challenge with Interoperability

Part of the problem is that it takes several parties and connected processes to conduct a transaction. The more equipment, software and so on involved, the more likely the vulnerability. Companies and entities have a lot to handle here, with so many requirements for digital and physical access. Yet identification of the person should be 'once and complete' if a system is to be used—especially with consumers. If the log in or check out with a favorite retailer is too complex, shoppers will abandon that merchant. The method of authentication is somewhat permanent and the customer authentication budget should reflect that. (Pin chip cards cost more than magnetic strips—but I will keep my credit card for five or more years and may use it for tens of thousands of dollars of purchases). Most retailers turn over the point-of-sale hardware in the same cadence, five to seven years.

In the same way, authentication of goods should happen quickly and easily (the speed of a conveyor belt), but unlike 'people identity,' it needs to be inexpensive, since there are so many goods and often the tag is only a one-time-use item.

Access

One other point is critical here as we think about interoperability: *access*. We don't expect the shopper to have access to all the corporate processes. Thus, their access is limited to a few processes. Conversely, employees may have more access and yes, they should comply with more 'layers' of authentication. The span of access varies greatly and unto itself can be fairly complex to manage: She can see this data—but not that. He can go into this building, not that section.

Interoperability

A benefit and a challenge. We need interoperability so systems can talk to each other. Interoperability has been created today (as in the credit card example above) with a variety of manual or automated methods. ID number, date of birth, security questions, and so on, are fairly standard, easy to implement, and effective. However, they often are not required. This probably needs to change to ensure access control.

---

manufacturing, supply chain and logistics, merchandising and so on tend to think that IT will address this problem. Yet they each have a large role to play and need to take ownership of the issues, since the partners, suppliers and supplies, and the processes they use will either enhance quality and security or reduce them; either make product processes safer—or not—for their customers.

Securing People, Goods, Systems and Processes

Federated Identity Management for Supplier Relationships

A bright spot has been the creation of a system and an infrastructure that federates a group of systems that deal with complexities of authentication and identity. One such example is Exostar. Exostar started out as an exchange system for big aerospace companies who had to integrate their supplier chains. Obvious security and authentication challenges arise in these relationships. Thus, the creation of Exostar's identity management solution

Exostar's federated identity management system addresses both physical and systems access for employees, suppliers, and partners. To quote the company in an interview we had, "What we're federating is identities to create a trusted environment of people, information, applications, etc. With that trust comes confidence that access can be provided securely because we have authenticated the identities of individuals."

This is a neutral third-party system that addresses the multi-layered and complex problems of both physical and digital identity and authorization.

Part of the complexity in the challenges Exostar addresses lies in enforcing the access privileges assigned by asset owners who connect their applications and information to the community, effectively allowing individuals to securely leverage third-party assets. Individuals gain authority to access third-party systems. Think about enterprises today. They are a complex web of both enterprise and third-party systems, i.e. your ERP systems have to access some supply chain, referential, or supporting systems that may be managed by others. Or your systems themselves may be managed by others. Or your employees are in remote locations, logging in from remote or third-party systems. It becomes clear that there are a lot of systems and interfaces. And again, employees and partners often have complex multi-layered access requirements. Having a third party manage all this complexity is an approach many enterprises are turning to. Exostar's *Identity Hub* has become popular with industries such as Aerospace and Defense, Life Science and Healthcare organizations such Merck AstraZeneca and companies such as Boeing and Raytheon that are well-known for requiring security across their supply chains.

Securing People Access

Another approach is IDV Solutions' Visual Command Center. Again, this provides the choice of the third-party neutral platform. This solution addresses the visual requirements of managing risks. A command center of security personnel can have visibility into processes and people in motion and see the environmental factors they are interacting with. Security personnel can see a real-time picture of the people and goods along with factors that impact their safety or security. It answers the questions of where and what kind of risk may be occurring at a location. It adds the 'physicality' to the picture—video—with RFID for access control and authentication.

Securing on the Road

What about in goods in motion—the grist of global transportation—ocean carriers and containers, rail and truck? Savi Technology has such an option. Savi's claim to fame is their RFID and Sensor analytic-driven applications that sit on top of a location/context-aware infrastructure. Remote or on-the-road

security and safety are addressed, seeing both item-level issues from the sensors—some event is happening to the item, and their context—where and under what circumstances that event is occurring. This is a more advanced approach to track and trace than just the 'slap and ship' approach of RFID alone.

There are many internet-of-things tools and platforms out there, but Savi's Insight is an application with already-developed uses cases and analytics for securing things in motion across the globe.

Your Digital Self

Part of our identity, since humans walked the earth, is our signature. Today, of course, we still value the signature above all else as our *authentic mark.* As more and more documents go online, the use of esignatures has also risen. DocuSign, the most sophisticated of this group of companies, has a vision—Digital Transaction Management—to support the growth of the digital enterprise.

Biometric systems have had troubled growth, but slowly continue to make progress. HID, a leader in authentication/access control technologies, recently has forged a path forward to add biometrics to their portfolio.

Sectors	Typical Companies	Commentary
Security Software	EMC/RSA, McAfee, Symantec, IBM, VeriSign	Account access (single sign-on), Encryption, Threat Management; Firewall Antivirus and anti-malware; IDS/IPS; Security and Vulnerability Management; DDoS; Web/endpoint authentication
Secure Managed File Transfer	Dell Boomi, Cleo, Ipswitch, bTrade, major EDI providers, Box, Hightail, Dropbox	Ensure secure data movement
Traceability, Tracking Software and Hardware	Savi, TraceLink	Item, shipment tracking and authentication
Supplier Relationship/ Supply Chain and Security Risk	Hiperos, Kroll/CVM, IDV Solutions, Resilinc, Zurich Insurance Group	Partner/Relationship authentication, security and risk management
Risk Monitoring Solutions		Today these are in many industries from financial sectors, weather, transportation, etc.
Integrated Identity Hubs	IdenTrust Trust Network, Exostar, Oracle	Combining various technologies to support the community/industry shared requirements such as financial/banking, supplier authentication, supply chain risk and so on
Smart Card, RFID chips/solutions	HID, Zebra/Motorola, SMARTRAC, Confidex, Impinj, Alien Technology	Security chips and tags for cards, access control, secured items

Figure 2: Sectors of Security and Identity

Into the Future—Identity Management, the Next "ERP"

The problem is vast, the challenges are tricky and the market is loaded with point solutions. Various ways to describe these sectors somewhat exist. (See Figure 2, above)

The security software solutions we are most familiar with are Symantec, EMC (RSA), McAfee, etc. These solutions were designed for system security, and their functionality continues to expand to include the system-to-system interactions for business and consumers. But there are a variety of other solutions that address both technology and applications which end-users may be more familiar with, such as supply chain risk management and risk management.

Various market 'names' define these sectors, such as Security and Identity Management, Access and Identity Management (AIM), eID and so on. Estimates vary on the combined size of these markets due to differences in definitions and lack of revenue recognition, but collectively, the market is more than $25B, not including consulting services.

However, any company needs these combinations of security, identity, and authentication methods (Figure 3).

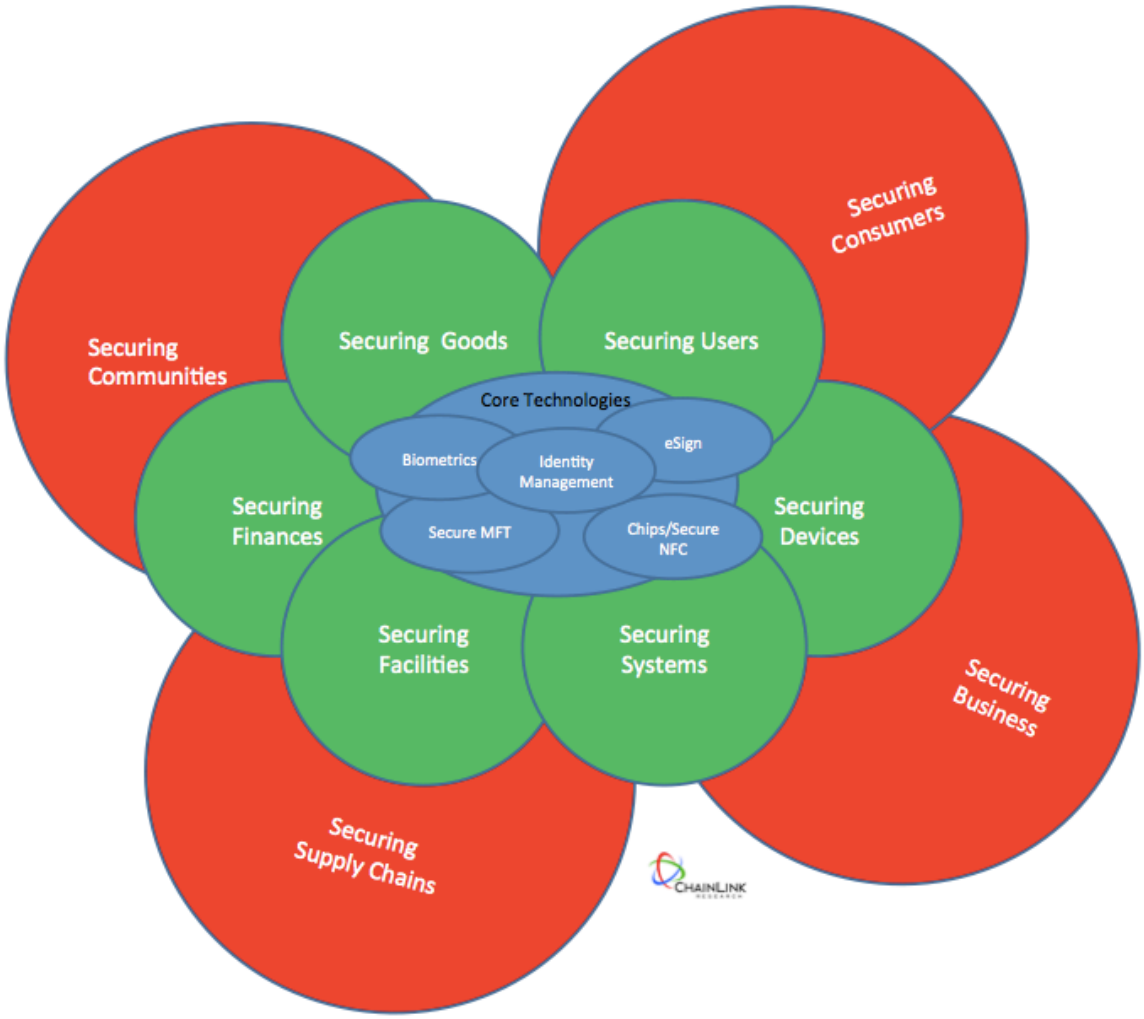

Figure 3: Security, Identity, and Authentication Used in Concert

What is *emerging is the understanding* by the user and technology communities that the problems of securing systems, processes, facilities, people and goods are somehow linked in the digital world. And that to fully solve the problems of identity and authentication, a multi-layered set of technologies is needed. No one thing alone will suffice.

So that is just why a company like Exostar has created their federated model, which brings together identity providers (including Exostar, trusted third-parties, and organizations participating in the community) and service providers (cloud-based and on-premises application owners including participating organizations, Exostar, and other third-parties). The result is a cloud-based community where governance and access rules are developed by the participants and enforced by Exostar, organizations can connect once, and users are authenticated and given single sign-on access to the assets to which they are entitled – bringing security and productivity to all cross-enterprise communications and collaborations.

Photo Art: © Ra2studio | Dreamstime.com

Authentication & Identity Solutions (AIS) (sometimes called Authentication and Identity Management) fill the needs of governments, businesses, and consumers. Most companies are depending on some level of security within their enterprise and infrastructure systems, so the providers of solutions such as ERP, Supply Chain, ecommerce, and financial systems could incorporate these AIS into their solutions, thus solving their own challenges of constantly keeping up with technology changes and integrations. Enterprise, as well, can access these solutions, especially through a SaaS service, which would make it easy for them to gain use—like a LifeLock/Life Alert type of solution that consumers have.

But the point is that there is a market for AIS and that the market will support many companies that offer AIS from a single portfolio provider (who has built or acquired most of the modules) or a federated system offering the vast suite of required solutions. We have already seen the hints of these united approaches emerging in the market. Uniting the point solutions under an umbrella offering will enhance—not reduce—the size of the market.

We think the problem is so big and so universal that just as the ERP market emerged from many point solutions to become an $50B market, so too will AIS. Other more clever names may emerge. But the fact is that the industry and its ecosystems of consultants, post-event investigators, audit and compliance (for PCS, ISO and other security and compliance stamps of approval) is already quite large by some estimates, probably doubling the size of the $25B. Companies will continue to seek new and better solutions—more extensions of what they already have—to stay ahead of the maliciously creative efforts of criminals.

Later this month we will expand on this model and explore the technology, companies, and users of these solutions.

References:

Supply Chain Risk Management Solutions
Risk Management collection
Security

Addendum:

- In January 2014, **Target** announced that an additional 70 million individuals' contact information was taken during the December 2013 breach, in which 40 million customers' credit and debit card information was stolen.
- **Neiman Marcus:** Between July and October 2013, the credit card information of 350,000 individuals was stolen, and more than 9,000 of the credit cards have been used fraudulently since the attack. Sophisticated code written by the hackers allowed them to move through company computers, undetected by company employees for months.
- **Michaels:** Between May 2013 and January 2014, the payment cards of 2.6 million Michaels' customers were affected. Attackers targeted the Michaels POS system to gain access to their systems.
- **Yahoo! Mail:** The email service for 273 million users was reportedly hacked in January 2014, although the specific number of accounts affected was not released.
- **Aaron Brothers:** The credit and debit card information for roughly 400,000 customers of Aaron Brothers, a subsidiary of Michaels, was compromised by the same POS system malware.
- **AT&T:** For two weeks, AT&T was hacked from the inside by personnel who accessed user information, including social security information.
- **eBay:** Cyber attacks in late February and early March 2014 led to the compromise of eBay employee logins, allowing access to the contact and login information for 233 million eBay customers.
- **P.F. Chang:** Between September 2013 and June 2014, credit and debit card information from 33 P.F. Chang's restaurants was compromised and reportedly sold online.
- **Community Health Systems (CHS)** warns that any patient who visited any of its 206 hospital locations over the past five years may have had his or her data compromised. The sophisticated malware used in the attack reportedly originated in China. The FBI warns that other health care firms may also have been attacked.
- **UPS:** Between January and August 2014, customer information from more than 50 UPS stores was compromised, including financial data, reportedly as a result of the Backoff malware attacks.
- **Home Depot:** Cyber criminals reportedly used malware to compromise the credit card information for roughly 56 million shoppers in Home Depot's 2,000 U.S. and Canadian outlets.
- **Google:** Reportedly, 5 million Gmail usernames and passwords were compromised. About 100,000 were released on a Russian forum site.
- **Apple iCloud:** Hackers reportedly used passwords hacked with brute-force tactics and third-party applications to access Apple users' online data storage, leading to the subsequent posting of celebrities' private photos online.
- **Goodwill:** Between February 2013 and August 2014, information for roughly 868,000 credit and debit cards was reportedly stolen from 330 Goodwill stores. Malware infected the chain store through infected third-party vendors.
- **SuperValu** was attacked between June and July 2014, and suffered another malware attack between late August and September 2014. The first theft included customer and payment card information from some of its Cub Foods, Shop 'n Save, and Shoppers stores. The second attack reportedly involved only payment card data.
- **Dairy Queen International (restaurant):** Credit and debit card information from 395 Dairy Queen and Orange Julius stores was compromised by the Backoff malware.
- **Dropbox:** Also had a major hack. Read Sorry, Dropbox.

