Tech Data 2011 Identity and Access Management Security Sales Toolkit:

How to build security offerings into your practice

Author: Mark S.A. Smith, OCE, Inc.
Editor: Kimberly Stagg, Tech Data Corporation
Subject Matter Expert: Matthew Dreger, Tech Data Corporation
OCE Project Manager: Debbie Albayati, OCE, Inc.
Project Manager: Effie Hayward, Tech Data Corporation

Printed in the USA
V1.0

Disclaimer
Neither the author nor the publisher assumes any responsibility for errors, inaccuracies or omissions. Any slights of people or organizations are unintentional.

This publication is not intended for use as a source of security, technical, legal, accounting, financial or other professional advice. If advice concerning these matters is needed, seek the services of a qualified professional as this information is not a substitute for professional counsel. Neither the author nor the publisher accepts any responsibility or liability for your use of the ideas presented herein.

Some suggestions made in this document concerning business practices may have inadvertently introduced practices deemed unlawful in certain states, municipalities or countries. You should be aware of the various laws governing your business practices in your particular industry and in your location.

Any websites referenced were personally reviewed by the author; there are no guarantees to their safety. Practice safe Internet surfing with current antivirus software and a browser with active security settings.

Tech Data 2011
Identity and Access Management Sales Toolkit:
How to build security offerings into your practice

Welcome to the Tech Data Identity and Access Management Sales Toolkit. As you expand your security practice beyond providing basic security management such as email and Web threats, you'll find this guide to be useful in dealing with more extensive security issues.

This guide contains many ideas that you can use to connect with your customer and illustrate that you know what you're doing when it comes to identity and access management.

How to Use This Toolkit

If you're new to identity and access management solutions, this guide is a great place to start.

If you've been selling identity and access management, use this document to make sure that you're covering all the bases. Most likely there are new ideas in this toolkit that you can use to enhance your practice.

While it's impossible to cover every aspect of identity and access management in this sales kit, Tech Data has a wide range of resources that can help you solve your client's problems. With staff subject matter experts and contact with top industry experts, we can help you find a solution. Please call us if you can't find what you're looking for in this sales toolkit.

Review and scan through this document looking for what's most interesting to you. By doing this you'll rapidly identify content that's new without wasting of time reading every word.

As you review this material, identify what you want to share with your staff and clients to help them have a more successful and secure operation. Doing this lets you get the most out of your time with the sales toolkit.

What is Identity and Access Management?

This guide reviews how to manage access to your customers' sensitive and valuable corporate data. Identity and Access Management combines three elements, authentication, authorization, and accounting collectively called AAA. Let's take an in-depth look at these three areas.

Authentication

The first step to access control is verifying an individual's identity, that a person is who they claim to be. If an attacker can't get past the authentication system, they can't do damage.

Authenticate by confirming something you know, such as a lock combination or a password; something you have, such as a key or ID card; or something you are or do, such as physical attributes or behaviors.

Something You Know

A password is the oldest and simplest way to identify friend or foe; just ask a question that only an authorized person can answer.

For example, financial institutions ask for your Social Security number, your mother's maiden name or a personal identification number (PIN). With the proliferation of social media and online sites for many people, these specific pieces of information can be found with a quick search.

Passwords

Your first line of defense against unauthorized access is a combination of user names and passwords, allowing authentication of individuals and providing a rudimentary level of non-repudiation. [1]

Passwords can be defeated by:

- The user disclosing to another their user name and password
- The information being observed as it was typed in (called shoulder surfing)
- Being found on a cheat sheet near the computer
- Being discovered by attackers with a dictionary attack or brute force attack [2]

Internal and External Passwords

When you access external systems or Web sites, your user name and password are often open to interception. For this reason, create policy to always use different user names and passwords for internal systems that are never used with external systems.

Other security experts recommend three levels of user name and password security: one combination for highly sensitive internal access, a second combination for offsite sensitive sites, and a third combination for sites with limited sensitivity.

Complex Passwords

Complex passwords are created by mixing upper and lower case characters, numbers and special characters to create a password that can't be found in a dictionary (like o0iCu812). [3] An eight character password like this generates 6,095 trillion possible combinations; you're pretty safe.

While they're complicated to crack, passwords like this can be unreasonable for users to remember. Each month, about 30 percent [4] of passwords are forgotten and manually reset by help desk personnel, with the greatest number on Mondays and after a holiday.

If users can't remember passwords, they'll write them down. The more often that a user is forced to change their password, the more likely they'll write it down. A written combination defeats security, even if it's stored in the bottom of a pencil holder, a common place to stash passwords.

Do a quick audit in your office; find out how many people have a sticky note with passwords on their monitor, hidden under their keyboard, or sitting in the top desk drawer. You'll be surprised.

Create Memorable Complex Passwords

You can create a complex password by using the first letter of each word in a memorable sentence. For example, "I love to ski and dive but not at the same time," yields Il2s&dbN@tst.

You can also create a complex password by simply typing in a short sentence. Another method is alternating the characters of two words into a single password. For example, blend MILK and eggs to create the password MeIgLgKs.[5]

Simple Passwords

Simple passwords, like a four-digit PIN, are easy for users to remember. While easy to crack, a short password is very secure when your system locks out a user name after a few log-in attempts. This is a common security method with mobile devices, such as smart phones. Yet, 54 percent of phones don't have password protection.[6] Make sure your clients have this simple policy in place.

[1] Non-repudiation means that you can't say it wasn't you that logged on with that combination.

[2] Widely-available tools such as crack and 11oft attempt to bypass log-in systems by trying frequently-used passwords from a dictionary, then resort to brute force by trying all other letter and number combinations.

[3] Read it out to hear the sentence. A classic complex password, this one happens to be in attackers' dictionaries so don't use it.

[4] Industry survey numbers range from 15 to 40 percent.

[5] Or to make an omelet.

[6] http://www.fastcompany.com/1766622/infographic-found-the-top-10-places-you-lost-your-smartphone

Password Policy

You clients need a password policy. Consider recommending the following tactics for creating secure passwords:

- Set policy that access to all personal computers requires a password.[7]
- Strictly prohibit users from giving others their password. Create guest accounts with very limited capability for casual users or visitors.
- Permit passwords that are simple to remember, but not the company name, user name, or other password that's easily guessed by a colleague.[8]
- Lock out a user name after four sequential failed attempts to prevent password cracking attacks.
- For network access, only permit a user name to be logged on in one location. This enforces not sharing user names.
- Use complex passwords for your servers and critical computers. Better yet, use stronger, two-factor authentication, discussed below.
- Train users how to create complex passwords that are easy to remember but hard to crack.
- Train users to choose different user names and passwords for external systems and Web sites to prevent internal access information from being accidentally disclosed.
- Require that laptops and PCs have complex passwords at boot up, securing the data if the computer is stolen. Don't rely on the operating system passwords after the system starts. It's very easy to crack these passwords. [9]
- Use a screen-blanking[10] screen saver with a simple password (one comes with Windows) to secure an un-occupied computer from an inside attacker. While rebooting easily defeats a screen saver, the attacker will have to re-log on to the computer with a password.
- A computer that's turned off is quite secure, so switch off workstations on weekends and holidays. Consider shutting them down at night.[11] Obviously this doesn't apply to corporate servers.

Single Sign-on

Single sign-on permits a user to be authenticated once to access multiple authorized applications. It eliminates future authentication prompts during that session when the user switches applications.

Single sign-on eliminates inconsistent password implementation between applications, keeps the password count to a bare minimum, makes it easy to authorize and immediately un-authorize a user, and saves time logging in and out.

Something You Have

Another way of verifying a person is by an article in their possession, such as an ID card or key. A unique item delivers a higher level of non-repudiation than just a user name and password combination.

Two-factor Authentication

Article-based authentication can be easily circumvented if the item is stolen or borrowed, so it's frequently used with a second method, creating two-factor authentication.

For example, a signed credit card (an article) and a matching signature (a behavior) allow a clerk to authorize a charge.[12] Or an ID badge (an article) with a photograph (a physical characteristic) gains access via a guard. Or your ATM card (an article) and your PIN (a password) gets cash for lunch.

---

[7] Most experts suggest changing passwords regularly. This becomes less important if you use the rest of these tactics.

[8] The most common passwords are admin and password. Most passwords are the names of pets, sports teams, children, family members, qwerty and 12345678. Go figure.

[9] Most passwords of up to 14 characters can be cracked in a few minutes by a widely available download. http://en.wikipedia.org/wiki/Ophcrack

[10] A blank screen saves energy and makes the computer appear to be off, further deterring internal attack.

[11] Most experts now agree that turning off a PC extends its life and delivers a 60 percent energy savings. The concern about damage on power-up just isn't valid.

[12] Payment processing guru, Dan Alcorn calls a family member's unauthorized credit card use loving fraud, as the victim refuses to prosecute the perpetrator.

Security Token

A security (or authentication) token is a small device such as a smart card[13], key fob or USB device that uniquely identifies a user to the security system.

Security tokens are often part of a two-factor authentication system with a user name or PIN that identifies the user as the owner of that specific device.

For example, RSA's SecurID gives users a key fob or credit-card sized device that displays a new six-digit code every 60 seconds. To log on, users enter the code along with their user name and password.

VeriSign offers their Unified Authentication managed service using USB devices. They manage the verification and infrastructure.

Secure Computing offers a SafeWord token that generates a one-time password on each touch of the device's button that's combined with a user name and PIN to authenticate access.

The most secure tokens become part of the user's guarded personal possessions, like their wallet for a smartcard or keys for a fob. If not, the token may be left behind, becoming useless to the user and potentially useful to the finder.

Controlling the Keys

While physical keys are not specifically an IT-based security solution, security policies need to address them, so here are a few thoughts to consider.

Secure physical assets with a lock and key. But the security is only as strong as the lock and as safe as the people you trust with the key. Commonly-held keys have a very low level of non-repudiation, so if you want auditable behavior, don't trust keys.

This is why many organizations have gone to an RFID badge entry system instead of physical keys. They know who has access, when they access, and can change access permissions in just a minute.

If your client is going to use physical keys, here are some tactics to increase key security:

- Check keys in and out. Have employees sign for each key and only give them a key if it's necessary to perform a daily task.
- Invest in high security locks available only from locksmiths with keys that aren't easily duplicated at the corner store. Mark them "Do not duplicate."
- If you have standard locks, re-key critical locks upon employee termination.
- Don't put identifying marks on keys. Never put your name, address or phone number on keys. Better to replace keys than have them returned by a thief, in person, at night.

Something You Are

The authentication method with the highest level of non-repudiation is based on who you are. Biometrics uniquely identify someone by measuring and analyzing unique human body characteristics such as fingerprints, eye retinas and irises, voice and face recognition, hand geometry, and even DNA matching.

Biometrics is going main stream as many enterprise laptop computers now come with a built-in fingerprint reader that replaces user passwords. Door locks with fingerprint readers can be had for less than $500.

[13] A smart card is a credit-card size device embedded with a data-filled microchip. Some require physical contact with a reading device, others can be queried remotely. More than a billion are used worldwide. One vendor is RSA Security.

Authorization
Authorization permits what a user can do. It enforces policies by allowing or disallowing the users' activities and privileges with resources, services, and data. Authorization should be set up by job function with a view to a user's roles and responsibilities.

For example, you may allow an accounting department employee access to financial records from their desktop during normal business hours, but disallow access with their user name from other machines or outside business hours. If they need to work after hours, you can set up a one-time user name and password to accommodate them, yet retain strong authorization control.

Another example, you may wish to allow a supervisor to view the files of their direct reports, but not make changes to basic information. Nor should they be able to view the files of other supervisor's employees.

Access to the highest level of authorization should be restricted to people who you trust completely, and should still be audited. As good policy, only allow top level access for the task at hand, logging in with lower authorization for routine tasks. The highest levels of authorization may require two people to gain access.[14]

Accounting
Accounting measures the resources consumed during access (such as computer system time used and how many data transactions occurred) supplying usage details for departmental or customer billing, and trend analysis for growth forecasts. Accounting also can monitor activity and track unauthorized access attempts, a behavior that is grounds for dismissal at many companies.

AAA Servers
A dedicated AAA server often delivers authentication, authorization, and accounting services. Most use the Remote Authentication Dial-In User Service (RADIUS) standard that maintains a central database of user profiles shared by all other servers. This makes it easy to enforce access policy across a wide range of applications and devices. For example, a single change to the AAA server database ends all computer access to a terminated employee.

While many clients will want to take a phased approach to identity and access management, this can be dangerous because it will potentially open security holes. It's much better to deliver all three of these elements in a single solution at once.

The Identity and Access Management Market Opportunity
Regardless of the size of the enterprise, the more mission-critical your clients data, the more they need identity and access management.

Business Drivers
The biggest business driver for Identity and Access Management is security and privacy mandates: federal, state, local, corporate and customer demanded policies. Once you understand the risks that your clients must manage, you can then determine the scope of the solution.

The problem is wide spread and worldwide. The Financial Times reports that 88 percent of companies in the US suffered some loss due to fraud in 2010, reaching 92 percent for those doing business in the Asia Pacific region. An amazing 27 percent of the companies interviewed reported theft of intellectual property by external hackers, disgruntled employees or foreign governments.[15]

[14] An extreme example, launching a U.S. ICBM requires two operators to simultaneously turn keys at independent workstations.

[15] http://www.ft.com/cms/s/2/4927f4e2-da1a-11df-bdd7-00144feabdc0.html#axzz1S1Hf8cVI

Some of the reasons for the attacks:

- Certain companies are targeting competitors in attempts to sabotage business or steal secrets, a behavior that increases during depressed financial times.
- Others want to gain notoriety in finding and revealing corporate dirty laundry in the form of WikiLeaks.
- Organized crime generates huge profits because stolen or pirated data can be immediately used for profits.
- Companies don't take security seriously, with a majority of SMBs not having a rudimentary security policy, making them easy pickings.

Ask your clients about their concerns, especially experienced executives who read the horror stories in the business papers every day.

Technology Drivers

There was a time when corporate espionage had limited value. You couldn't hijack a filing cabinet and one could only photograph so much during a stealthy night raid. The vast majority of corporate value now resides in electronic databases: intellectual property, trade secrets, customer lists and historical data. Virtually all of this data resides in electronic format on disk drives—both on servers and personal computers—and backup tapes often scattered throughout the organization.

A disgruntled employee with a USB drive can commandeer a car load of intellectual property and trade secrets. Once they leave the property, there is not much that can be done to recover them. Sure you can sue, but that could take years and the damage can be beyond recovery.

While it's important for trusted employees to access the information required to effectively do their job, it's also important to limit access to only those who need the information. If your customer hasn't updated their database access strategies, it's possible that any employee can walk up to the right computer during lunch, and 10 minutes later have the entire corporate database on a portable disk drive.

Do you sense a business opportunity here?

Future Trends

The trend of espionage from foreign governments, organized crime and competitors will continue. It's just too profitable and too tempting; the odds of getting caught and the costs of being caught are low. Expect more infiltration from outside organizations looking to profit from corporate data.
Here are some threats to be looking for:

- Organized crime gets more aggressive about placing people inside organizations to steal data and then disappear, especially financial institutions.
- Disgruntled employees being courted by competitors, leaving with a memory stick full of sensitive and valuable corporate data.
- Expect more mandates for information and data access control from all fronts.

How to Identify Likely Prospects for Identity and Access Management

You can identify opportunities for your security practice by asking smart questions and intelligently identifying what security topics to discuss with your clients.

Qualifying Questions for Identity and Access Management

These questions let you examine your client's current security situation to determine if expanding their security makes sense.

- How do you control access and audit activities around your critical data?
- What would happen if critical customer data got the hands of the wrong people?
- How will you keep this from happening?
- What are your plans to protect sensitive data safe when accessed via mobile devices?
- What levels of access control are you required by law to maintain?
- What is the potential legal exposure if your organization inadvertently permits access to someone unauthorized?

Aligning with Your Client's Motivation

There will most likely be a number of people involved in the decision-making process. You'll need to satisfy the executives' concerns, the technical requirements of the IT department, the mandates of the legal department, and the HR department may have an opinion on issuing secure name badges.

Each of these players in the decision-making process has their own view of what's important. For example, the IT administrator will focus on making sure the security solution won't impact the IT operation. They will also want to know the nitty-gritty details about how you plan on delivering the solution. The legal department needs to make sure that they are covered in case of a breach so that they have legal defense if they're brought to court or have evidence when they need to take someone to court. The executives want to make sure that they can maintain and grow operations with minimal risk. Customers want to make sure that their proprietary data stays private.

This means that you need to cover each of these motivating factors of the decision-making team during the discussion of your proposed solution. Now that you understand some of the issues and motivating drivers for your client, you can be very compelling as you position your security offerings.

Illustrating Compelling Value of Identity and Access Management

When you choose a vendor (with the help from your Tech Data Sales team) for deploying Identity and Access Management solutions, you'll frequently be able to us specific tools that will help develop strong value propositions to share with your clients.

Couple this with the research that you've done by asking the questions discussed above and you'll be able to present a compelling reason for your clients to take action now.

You can calculate what a data breach costs for your clients with the Ponemon Institute/Symantec Data Breach Risk Calculator.[16] You can also get current comparisons with others in the industry to benchmark data risk costs from this resource.

[16] http://databreachcalculator.com

Who to Talk With: Getting to the Decision-Making Team

The secret is to identify who is most at risk when information becomes compromised. Depending on the relationship you have with your clients, you may already have access to the key decision-makers. Or you may need to establish new relationships higher up in the organization.

The responsible party could have a title such as CIO, security officer, legal officer, IT administrator, compliance officer or similar title.

In any case, you can most efficiently find the security decision-maker by asking your contact the question, "Who is responsible for data access security?"

If the person you're speaking with isn't responsible, they will gladly point you in the right direction. And who can blame them? They don't want the responsibility.

Ask your contact to make the introduction. If that's not possible, or you don't have a contact in your target customer, you'll have to get their attention on your own.

Suggested Introduction Email:

Identity control and access management concerns

Appleseed, John <John.Appleseed@techdata.com>

To: Myia Client <m_client@aol.com

Did you know that 27 percent of companies worldwide have critical information stolen from them every year? What do the other three quarters of the companies know that these companies don't?

The answer is they know how to manage access. If this concerns you, let's talk. If not, would you let me know who should be concerned?

I am (your name) with (your company). Our clients tell us that they work with us because they can let us worry about security issues so that they can go about what's important in their business.

Please let me share with you some things we've done for our clients and identify if we can help you in a similar way.

Just drop me an email to schedule a time to speak or call my cell phone at (your phone number).

P.S. You might find this information helpful. (Web address for additional information about your security services.)

What to Say: Aligning with Their Motivation

In your conversation with them, confirm they are indeed responsible for data security and then ask them, "How do you plan and budget for identity and access management?" This will give you some insight in to how they approach their job. If they aren't responsible for planning and budgeting, they are the wrong person to speak with. Find out who is and get to them.

Follow-up with the question, "How would you like that to change?" What they want to change is what they're willing to buy. Now it's just a matter of matching what you have to offer with what they'd like to do differently.

Managing Common Objections

No doubt you'll run across some objections when you talk with your customers about identity and access management solutions. Here are the most common ones that show up and some suggestions on how to manage them.

The most likely objection that you'll hear is, "Our systems are already secure."
Your response to this should be, "I'm sure they are! Yet what happens when you need to fire a critical employee? How quickly can you protect your critical data from misappropriation? Let me take a look at your systems to look for gaps. If we find anything, it'll save you the cost and embarrassment of an attack. If we don't find anything, you can say that you're just being cautious and exercising reasonable care."

Another common objection is, "We don't have the money."

I'm sure you hear this all the time. Next time you do, try this reply: "I totally understand. Yet what have you budgeted for when someone gets a hold of information that they shouldn't? Your company probably has an employee handbook full of codes of conduct. What are you doing to ensure that conduct and protect your critical assets? Let's take a look to see what it would cost if somebody accessed information they weren't supposed to and what it would be worth to prevent that from happening."

Closing the Deal
You may have noticed that this type of security project has more executive involvement than other projects. This means you'll need to work with the executives to identify execution plans and externally driven deadlines.

Align with their internal deadlines. If the CEO has promised a key customer that an access control security solution will be implemented in the next six months, use this information to your advantage. Any time that you can link your proposal to meeting internal deadlines, the deal goes fast.

Expanding the Identity and Access Management Opportunity
The process of delivering security services is similar to delivering any other technology. Break up the task into manageable chunks and just get started on the most important pieces.

It all starts with a review or creation of security policy. See the Secure Content and Threat Management sales kit for a discussion about creating security policies. Ask your Tech Data Sales team for a copy.

Begin by reviewing what level of security your client needs, then identify the barriers to making that happen. Next, assemble your team to craft strategic approaches to eliminating the barriers and evaluate potential solutions. Use the smart questions in this and other Tech Data Sales Kits that uncover the necessary information so that you can make intelligent choices, balancing risk and reward.

Likely Cross-Sell and Up-Sell Options
There are plenty of other items to sell your clients as you review their security situation. We have created sales toolkits to help in a number of these areas. Check with your Tech Data Sales teams for these sales kits:

- Application and Data Security
- Secure Content and Threat Management
- Security Compliance and Vulnerability Assessment & Management
- Video Surveillance

Your clients will also potentially need additional hardware appliances, networking, upgraded storage and improved data center physical security.