Tech Data 2011 Secure Content and Threat Management Security Sales Toolkit:

How to build security offerings into your practice

Author: Mark S.A. Smith, OCE, Inc.
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
Secure Content and Threat Management Sales Playbook:
How to build security offerings into your practice

Welcome to the Tech Data Secure Content and Threat Management Sales Toolkit. As you expand your security practice beyond providing basic and application threat management, you'll find this guide to be useful in dealing with more extensive security issues.

There are plenty of ideas in this guide that you can use to expand your practice. You will find best practices that will help you connect with your customer in a way that helps them see the value of what you're offering them.

How to Use this Toolkit

If you haven't delivered secure content and threat management solutions to your customers in the past, you'll find this guide will help pave the road to a successful expansion of your practice.

If you've been selling content security and threat management in the past, you'll want to use this guide to make sure you're delivering best practices. Without a doubt, there are some ideas in this toolkit you can use to improve the efficiency and profitability of your security practice.

Threat management is a moving target because the attack vectors and mitigation methods evolve rapidly and sometimes it seems difficult to keep up with all the changes and innovations.

While it's impossible to cover every aspect of content and threat management security in this sales kit, Tech Data has plenty of resources that can help you solve your client's problems. From on-staff subject matter experts to connections with top industry experts, we can help you find a solution. If you can't find the answer you're looking for in this sales toolkit, please call us.

You can get the most out of this sales toolkit by thumbing through, reading the headers, and looking for something that will grab your attention. The way that a trained technical brain works is it looks for knowledge gaps, so scanning through the content is the fastest way to add to your insights and grow your security practice.

As you review this content, use your best judgment to identify what will work for your company and your clients.

What is Secure Content and Threat Management?

In the Tech Data Application and Data Security Sales Toolkit (ask your Tech Data rep for a copy) we discussed how to implement fundamental security measures for and protecting applications from web-based threats.

In this guide will discuss how to manage other security threats such as external network-based attacks, internal data misappropriation, and data loss prevention (otherwise known as DLP).

Some of the technologies that can mitigate these security threats include intrusion protection systems (IPS), firewalls, and DLP technology. We'll also discuss other aspects of network security.

It's About Protecting the Data

For most companies, their greatest assets, after customer loyalty, are digital. According to a University of California study, 93 percent of information created by corporations is now in electronic form.

Even if your clients don't have competitors that choose to aggressively pursue industrial espionage, their network will be under attack with criminals looking for ways to break in and steal critical client content that they can use to their own advantage. Bad guys want to crack the company vaults and help themselves to valuable data and salable customer information.

Secure Content and Threat Management is about protecting those assets. There are advanced technologies to protect your client's data from network-based attacks. The challenge is that the criminals are getting more cunning and more clever about how they clandestinely attempt to crack your client's critical infrastructure.

Although the usual attack vector is with malware (such as viruses, Trojans, worms), payloads (scams, phishing, spam), or weak protection from unauthorized access, increasingly network attacks come through denial of service attacks and harvesting attacks from botnets created from worms.

Worming into the Network

Now more common than viruses, a computer worm is malicious code that does no harm to the host, but secretly invades and takes over the computer to do the nefarious bidding of its creator, like a zombie. A worm silently propagates through network and Internet connections. They try to remain invisible and are often only noticed when the infected computer slows to a crawl, when an antivirus scan detects it (more difficult to do these days), or when an intrusion prevention system spots unexpected or abnormal activity.

Zombie Computers Arise

These zombies form a botnet, a network of clandestinely controlled computers sending spammer's s or leveling other attacks. Botnets are used to launch a directed denial of service (DDoS) attack on a Web site or server. A botnet bombards the target site with Web page requests or spam, overloading the server, making it unavailable for legitimate users. Think of DDoS as creating a computer busy signal.

Every day thousands of botnets spew out hundreds of thousands of spam messages or spawn other attacks. [1]

If your clients think that they are immune from these attacks, think again. Businesses as obscure as gold-mining and winemaking have endured packet-flooding attacks from malware-infected zombies. Other targets have included gaming sites and online stores. [2]

Harvesting Addresses

Botnets can instigate directory harvest attacks (DHA) to gather addresses. Spammers direct messages at a company using a dictionary of common names, collecting addresses that aren't rejected. A successful attack nets thousands of fresh addresses in minutes. That's why you can establish a new box and almost instantly get spam.

During a DHA or DDoS attack, your client's service slows substantially, inhibiting legitimate message delivery because the server responds to each message sent to an unrecognized address.

Botnet Defense

Protecting against DDoS attacks requires protection at the entry point of the network, usually with a dedicated appliance such as a firewall or intrusion prevention system (IPS). This device must be able to rapidly differentiate between authorized access and external attack.

For endpoint devices such as PCs and mobile devices, software can perform the function of a firewall or IPS. This approach usually impairs performance somewhat and requires regular updates as threats change. Software-based protection is mandatory if devices are used outside of the corporate firewall.

[1] See one source of frequently-updated botnet statistics at http://botnet-tracker.blogspot.com

[2] http://www.theregister.co.uk/2011/03/09/gold_mine_site_botnet/

Preventing Data Leaks

If data is the lifeblood of your client's business, then any data that leaks out saps the health of the organization. This data could be in the form of in trade secrets, problems with specific customers that may prove embarrassing, or information about future products that could undermine market success. These data leaks could be inadvertent or intentional, sloppy business practices, or industrial espionage.

Data Loss Prevention (DLP) systems are designed to detect and prevent unauthorized use and transmission of confidential information. DLP uses data systems that identify, monitor, and protect data in use (at endpoints such as PCs and mobile devices), data in motion (transferred over the network), and data at rest (data being stored) through deep content inspection and usage analysis managed by a centralized framework.

For example, if records about a new product release are being accessed at 3 AM by an unrecognized IP address, the odds are high that's unauthorized usage. That request gets challenged or blocked. Or your client may want to stop an instant message heading out of the firewall that contains a new product code word.

DLP solutions use multiple methods for content analysis, ranging from keywords, dictionaries, and regular expressions to partial document matching and fingerprinting. Most DLP are delivered by a combination of software solution, hardware appliance, or now more frequently, cloud-based services.

Software is often used on endpoint devices to detect data leakage. This requires maintenance and regular upgrades of the information signatures to be detected, and can be a challenge to implement on mobile devices such as cell phones.

Appliances and server-based software are used for detection of data leaks on the network or residing on storage devices.

The first step to a successful DLP solution is to have a written data security policy. Without a policy you have no idea how to set up a system to protect your client's critical and sensitive data. More about this later in this sales toolkit.

While automating a DLP solution is complex and requires a lot of maintenance, the cost or damage of a data leak to an organization is often orders of magnitude beyond the cost of a DLP solution. Explore these costs with your client to identify the value of a DLP solution, and you'll be very successful.

Customers and Courts Expect Compliance

If you've ever talked with a client who has experienced a malicious attack, you know that rarely are they surprised by the intrusion. Often they knew they had a weakness but hadn't gotten around to implementing a security solution. The cleanup process was expensive, time-consuming, and embarrassing.

If your client does business with a sophisticated business customer, they probably have a contract in place that specifies the security procedures for proprietary data. This is certainly true if your clients do business with state, local, or the federal government.

When it comes to data protection, ignorance is no defense. The bar is being set higher as to what constitutes reasonable care in providing security for customers, employees, and their data. If there's a security breach in your client's company, they can count on being asked tough questions by stakeholders and the law.

The odds are good that your client needs an outside, third-party to help them illustrate that they are using reasonable care in the protection of their data assets.

How this Landscape is Changing

Look for an increased number of attacks coming from smart phones attaching to corporate networks via Wi-Fi.
According to a recent Juniper study, which analyzed malware detected on its customer devices in 2010, smart phone spyware accounted for 61 percent of all mobile customer infections and 100 percent of all infections for Android devices. The report also documented a 400 percent increase in Android malware, as well as highly targeted Wi-Fi attacks. [3]

Why a Security Practice is Valuable for You

When you choose to expand your security practice to include secure content and threat management, you're moving into a bigger world with bigger projects and bigger clients with bigger stakes at risk. You'll also be involved with the important decision makers in your client organization, especially if you work with data leak prevention.

Business Requirements to Successfully Sell Secure Content and Threat Management Services

To sell these more advanced security services, you'll need to train your staff on how to conduct assessments, identify opportunities, and deploy sophisticated security technology. The good news is that you can charge nice fees for delivering the services, and in the process of doing so, more deeply entrench yourself into your client's organization.

Think about it this way: when you're working with your client's sensitive data, future plans, and proprietary materials, you become a true trusted advisor.

If you're like many business partners, you'll find that as you expand your security practice, the rest of your business grows organically as you add more services and products based on discovering what your clients really need.

The Secure Content and Threat Management Market Opportunity

Most of your clients have some type of security solution, even if it's just the free antivirus package that came with their computer. The problem is that while it's a good start, it's not enough. If they're likely to come under attack or be severely impacted by the leaked data, they need to expand their protection strategy.

Business Drivers

DDoS attacks designed to disable companies e-commerce are the modern equivalent to a mob shakedown—potentially forcing businesses to their knees. They've been around for a decade but are becoming more frequent and aggressive. [4]

And no business is immune: The actions of hacker group, Anonymous (particularly against Scientology) are well documented. In October, 2010 DDoS attacks occurred almost daily on the likes of the UK Intellectual Property Office, the US Copyright Office and KISS bassist, Gene Simmons' websites. More recently, Wikileaks, MasterCard and PayPal have been under attack.

While not a direct impact of DDoS – such attacks can serve as a diversion while infiltrating servers in the organization and wrecking havoc – compromising sensitive information, planting malicious code and more. So IPS and DLP go hand in hand.

As bad as DDoS seems, data loss can be more severe and costly. Consider the recent data leakage from SONY's PlayStation credit card transactions, losing control of 70 million records. Although their terms and conditions claim no liability for data loss, they are being aggressively sued on many fronts over the slip up.

[3] http://searchsecurity.techtarget.com/news/2240035699/Juniper-Networks-finds-rise-in-Android-phone-malware-smartphone-spyware

[4] http://thenextweb.com/media/2010/12/19/how-ddos-attacks-became-the-frontline-tool-of-cyber-war/

Industry analyst, Gartner estimates that 70 percent of corporate break-ins are motivated by money or political reasons. The other 30 percent are random attacks to grab whatever unsecured assets are available and cash in on your client's hard work. Attacks can come from innocently browsing the web. One out of 14 web downloads are malware. [5]

According to a recent survey by Cisco: [6]

- 33 percent of IT professionals were most concerned about data being lost or stolen through USB devices.
- 39 percent of IT professionals worldwide were more concerned about the threat from their own employees than the threat from outside hackers.
- 27 percent of IT professionals admitted that they did not know the trends of data loss incidents over the past few years.

You have a golden opportunity to educate your clients about these issues. They need to know about them and they should be hearing about them from you.

Technology Drivers

As compute power increases and high-speed bandwidth becomes ubiquitous, expect more threats to emerge targeting more and more organizations.

As new data protection mandates increase the retention time for data, the need for protection against data loss increases because there is so much more data at risk.

Threats will increasingly come from smart phones as they increase in compute power, essentially becoming a portable botnet.

Future Trends

The bad guys trying to get to your clients data are way more sophisticated than most of your clients. It's more cost-effective for organized crime to steal and resell data than it is to perpetrate personal attacks. Here are some threats to be looking for:

- Using social media opens up additional security holes for data leakage. While many companies block Facebook and Twitter, users can still get around these by using anonymizer websites. Look for ways to allow social media to be appropriately used as well as secured.
- New, online applications are constantly being created that will increase the potential for data sharing and increased security risks. Look for ways to balance the advantages of new applications with the need for security.
- As bandwidth demands increase, the network traffic scanning strategies must keep pace with the data throughput.

[5] http://www.zdnet.com/blog/networking/one-in-fourteen-internet-downloads-is-windows-malware/1079

[6] http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html

How to Identify Likely Prospects for Secure Content and Threat Management

When looking for security services opportunities, you can begin your reconnaissance by asking everybody you speak with, "What is your biggest concern about network security, specifically loss of service and leakage of data?"

The reason why this question works so well is because almost everybody has a difficult time keeping up with security issues. What you learn from this question will give you insights into where to probe further in your client's organization.

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

You may already have access to the decision-making team because of your client relationships. Or you may need to find some new contacts if you want to sell them security solutions. The first step is to identify who is impacted when systems are unavailable or there is a security breach. It doesn't make sense to talk to anyone else to begin with.

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 security?"

If the person you're speaking with isn't responsible, they will gladly point you in the right direction. Hey, they don't want to be responsible if they don't have to be.

How to Get the Meeting

Ask your contact to introduce you to the responsible party. If that's not possible, or you don't have a contact in your target customer, you'll have to create your own introduction.

Suggested Introduction

New Security Threats

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

To: Myia Client <m_client@aol.com

It's amazing that a famous, successful company can lose 70 million customer records to a hacker. This means the average technology user can't hope to keep up with the onslaught from the bad guys.

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 the 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.)

Suggested Voic Script

I'm (your name) with (your company). I've been working with technology for a long time and yet I've never seen anything like the number security threats hitting the network. For example, a Fortune 500 company can lose 70 million customer records to a hacker. This means the average technology user can't hope to keep up with the onslaught from the bad guys.
The purpose of my call is to share with you some ideas that I've found to solve this problem. Our clients tell us they choose to work with us because they can let us worry about these issues so that they can go about what's important in their business.
Please let me share with you some the things we've done for our clients and identify if we can help you in a similar way.
Just drop me an at (your address) to schedule a time to speak or call my cell phone at (your phone number).
I'm looking forward to sharing what I've learned, (their name).

What to Say: Aligning with Their Motivation

In your conversation with them, confirm they are indeed responsible for data security and then asked them, "How do you plan and budget for data security?" 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 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 security 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 when was the last time your system was tested? New threats come along every day and it only takes one that you're not protected against to destroy everything that you've done so far. We'll be glad to do this for you and 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 hear that all the time. And I'm sure you do, too. Yet what have you budgeted for when your security system fails and you have to recover from an attack? Your company probably retains lawyers and hires locksmiths to keep it safe. Yet your most valuable asset is your data. Let's take a look to see what it would cost to protect your data the same way you protect the rest to your company."

Yet another common objection is, "We're going to be looking at that in the future."

Try this response: "That's a great idea! How do you plan to protect your data between now and then? Let me at least put together an interim plan to keep you protected until you can put together a full solution."

Exploring the Secure Content and Threat 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 Secure Content and Threat Management

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

- If your data system was disabled, either from an intentional attack or an accident, how confident are you that you could quickly restore critical business systems before there was substantial impact?
- 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?
- How long do you have after a data breach or outage before your customers would begin looking for other vendors?
- What records are you required to maintain by law?
- How rapidly is this database growing?
- How are you assuring that these records are secure?
- What is the potential legal exposure if your organization cannot fulfill contractual obligations?
- What would happen if your company's financial records were destroyed? What would that cost?
- What incidents have you planned for?
- When was the plan last reviewed?

Triage Questions: Deciding What to Discuss for Greatest Impact

When it comes to security, there are so many things to talk about that you may be uncertain where to begin. Use this guide to identify where to start the conversation with your client.

What is your data security policy?

If they don't have a security policy, it's going to be very difficult to identify the holes in their security beyond the basics. Your first step will be to help them develop a policy that can then be enforced. Many of your clients will need help developing a security policy that includes secure content and threat management elements.

When was the last time your security policy was reviewed?

Even if the organization has a security policy, the odds are good that it hasn't been reviewed or tested since it was created. The next step is to evaluate the policy to identify where it needs to be revised and where there are implementation holes. The powerful thing about this approach is that management has already agreed to the policy, now it's just time to fund the implementation. You don't have to sell them anything, they just need to buy what they've already agreed to.

What is your biggest concern around data security?

Where your client has a concern, they know that there is a weakness in their security strategy. You can help them explore the costs of securing this weakness and identify the value of managing the issue.

What is your roadmap for securing your data?

If your client has an idea of where they want to go, your job is going to be easy. If they don't have a roadmap, you can consult with them on their security goals — based on corporate and legal mandates — and help them figure out how to get there.

Aligning with Your Client's Motivation

When you work with your client, there will most likely be multiple people involved in the decision-making process. You'll need to satisfy the concerns of the executives, the IT department, the legal department, and your client's customers. Each of these people has their own view of what's important in the decision-making process.

For example, the IT administrator will focus on making sure the security solution is going to be effective with limited impact on the rest of the IT operation. They will also want to know how you plan on delivering the security 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. The executives want to make sure that they can maintain and grow operations with minimal risk. The 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 position your security offerings in a way that is compelling.

Communicating Powerful Value Propositions

If your key contacts are in the IT department and they ask you for proposal, that means they are interested in your offering but they need to communicate the solution value to the rest of the decision-making team. Your proposal must include value propositions that appeal to the decision makers and the information that the proposal requires to say yes.

When creating your proposal, focus primarily on outcome instead of methodology. The reality is that in security, the methodology will change because the nature of the threats change. Instead, focus on how you will actively help your client protect their data and mitigate any issues that might arise.

If the IT administrator needs additional information about the methodology, include that as an appendix consisting of data sheets and white papers provided by the vendors you've selected.

Illustrating Compelling Value of Secure Content and Threat Management

When you choose a vendor (with the help from your Tech Data Sales team) for deploying threat management and content security solutions, you'll frequently get access to 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.[7] You can also get current comparisons with others in the industry to benchmark data risk costs from this resource.

Closing the Deal

Using the selected solution's TCO or ROI calculator you can figure the value of the security solution you're proposing. If you're calculating TCO, divide the resulting number by 36 if it's a three-year figure, or by 60 if it's a five-year estimate. This gives you the monthly savings for the solution. Use this number to illustrate the value of making a decision sooner instead of later.

For example if the security solution you're recommending saves them $30,000 a month, every month they delay the decision means they write an unnecessary check for $30,000.

Align with their internal deadlines. If the CEO has promised the Board of Directors that a 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, you will speed the deal.

[7] http://databreachcalculator.com

Expanding Secure Content and Threat Management

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.
Begin by reviewing what level of security you need. Then identify the barriers to making that happen. Next, assemble your team to craft strategic approaches to eliminating the barriers and evaluate potential solutions. Create smart questions that uncover the necessary information so that you can make intelligent choices, balancing risk and reward.

Services

Here are some of the services you can offer to your clients. Pick and choose those that you feel will enhance your business.

Creating, Reviewing, and Auditing Security Policy

Security strategy is based on policy, education, technology, measurement and enforcement. You can deliver services in each of these areas.

A policy is a document that summarizes requirements and prioritizes expectations that must be met for specific areas of the company. It details what's authorized, what's unauthorized, when policies apply, and who is responsible for maintaining and enforcing the policies.
A standard is a specific technical requirement that must be met by everyone. For example, a computer must be in a specific, secure configuration before connecting to the corporate network. Following industry standards provides a level of indemnification when a contract demands reasonable care.

A guideline is a recommended best practice that becomes established through experience. Effective security policies use existing standards and guidelines. This speeds adoption because it capitalizes on the corporate culture.

Start by creating a policy that defines roles and responsibilities. It's easier to write and approve a three-page document than a 200-page tome. Keep it short and focused, assigning responsibility to the right people and moving implementation details to the right level of expertise.

Classic policy details scope, reasons, definitions, domains, roles and responsibilities, management, documentation, implementation, measurement, and updates and changes.

Sample Policies

A quick Web search of "sample security policies" turns up a number of free and for fee examples.
SANS offers sample security policies developed by a group of experienced professionals; a good starting point. [8]

The IT security policy for Murdoch University in Australia is a tight document covering the key points, including permission for use by others. [9] You might use other university sites for policy examples. Just make sure that the policies are in the public domain so that you can use them.

The SAFE Blueprint from Cisco Systems is a best-practices technical discussion about business computer networks. It takes a defense-in-depth approach so the failure of one security system won't compromise the rest of the network. Although the recommendations are product agnostic, the solutions center on products from Cisco and partners. [10]

An expensive but widely regarded book, Information Security Policies Made Easy includes electronic templates and fully-developed examples. [11]

[8] http://www.sans.org/security-resources/policies/
http://www.murdoch.edu.au/index/policies/it
[10] http://www.cisco.com/go/safe
[11] http://www.amazon.com/Information-Security-Policies-Made-Version/dp/1881585131

Education

Security breaches begin with, “I don’t have to worry about a password; I only use the network for printing.”
The biggest bang for the security buck is educating your client’s people because it puts security into action. Educate all employees and vendors about security procedures and consequences of non-compliance.

Yes, this costs money, but so does insurance and the legal team. Some managers complain, “If I train them, they’ll just leave.” Well, what if you don’t train them, and they stay?

Most education is simple, like reminding employees to not discuss sensitive procedures with outsiders. Teach them that security is a group responsibility; a chain is only as strong as its weakest link.

You can either purchase security training sessions or develop your own proprietary materials based on the needs of your client.

Measurement

It makes no sense to have a policy that’s not measurable because no one knows how well they’re doing or where they need to improve.

Some things are easy to measure, for example your client can survey who’s wearing an ID badge and who has access to sensitive information.

Software tools can measure company-wide security policy compliance and can tell you how secure your client’s premises are. (We will cover that in another Security Sales Toolkit.) Many of these tools come pre-configured with security policies based on standards and best practices, making policy easy to implement and measure.

Audits

Your clients need a regular, third party audit to illustrate that they are in compliance and to illustrate best effort. You can regularly audit access to confidential information to determine how vulnerable your clients are. Review what information is accessible, by whom, and where and how it is accessible.

You can purchase tools that help with the security audit process. In addition you’ll find a similar security sales toolkit written specifically about security compliance and vulnerability assessment and management.

Enforcement

Few people want to play the heavy in enforcing security policy. Yet, a policy without enforcement is a set up for major trouble. You, as a third party, can help with this.
Rules and polices don’t have the force of law. Your clients can’t physically detain someone because they broke a corporate rule unless it’s backed up by legislation. But they can be dismissed.

One of the easiest ways to enforce policy is to show your clients how to make security compliance part of the regular performance review process. A good worker who isn’t safe isn’t good for the company.

Devise a series of warnings with increasingly stiff sanctions. Some infractions need to carry the penalty of instant dismissal, such as committing felonies on company property. Your client may wish to create rigorous responses to seemingly minor security infractions if those lapses result in legal exposure.

If a client’s employee, vendor, or customer breaks the law, call law enforcement.

Likely cross sell and up sell options

There are plenty of other items to sell your clients as you dig into their security requirements. We have created sales toolkits to help in quite a few of these areas. Ask your Tech Data rep for these sales kits:

- Application and Data Security
- Identity & Access Management
- Security Compliance and Vulnerability Assessment & Management
- Video Surveillance

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

Supporting Resources

There is certainly much more to discuss then we can cover in this sales kit. Use these resources as a good starting point to gather what you need to expand your security practice.

Industry Resources

Look at these web sites for sources of up-to-date statistics, ideas, and insights.

National Vulnerability Database

nvd.nist.gov – National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data.

The SANS (SysAdmin, Audit, Network, Security) Institute

www.sans.org/top-cyber-security-risks – SANS is a great resource for computer security training, network research, and resources.

Hoax Reference Site

Nothing kills your credibility faster than sharing bad data. http://snopes.com is the first stop for a quick check to see if a warning or story is hoax.

The Security-Specific Search Engine

SearchSecurity.com – Offers a variety of newsletters or Web casts dedicated to security. The site offers security-specific daily news, thousands of links, and interaction with leading industry experts.

Security and Privacy Research Center

www.cio.com – From creating and implementing a security policy to dealing with rogue programmers, the CIO Security and Privacy Research Center can help with ideas to keep a network and site secure.

Computerworld Knowledge Center

www.computerworld.com/securitytopics/security – Leading with the latest security headlines, Computerworld's site includes upcoming events, links to vendors, security statistics and reviews, as well as online discussions.

Electronic Privacy Information Center

www.epic.org – This site from the Electronic Privacy Information Center (EPIC), a public interest research center, covers the gamut of online privacy issues.

Computer Security Institute
www.gocsi.com – Publishes the annual FBI/CSI computer crime and security survey. Educates computer and network security professionals about protecting information assets.

The CERT Coordination Center
www.cert.org – Web site for the CERT Coordination Center at Carnegie Mellon University, a major reporting center for Internet and network security vulnerabilities.

Information Systems Security Association
www.issa.org – A non-profit association for information security professionals that facilitates interaction and education to promote secure information systems management practices.

Center for Internet Security
www.cisecurity.org – CIS members identify security threats of greatest concern and develop practical methods to reduce the threats. Provides methods and tools to improve, measure, monitor, and compare the security status of your Internet-connected systems and appliances. CIS is not tied to any specific product or service.

NIST's Computer Security Resource Center
csrc.nist.gov – Resources from the National Institute of Standards and Technology's Computer Security Division.

Assessment Tools
Most security vendors include a vulnerability assessment tool as part of their suite of products or as a sales tool. Ask them about what they have available for you to complement any tools you already have.

Tech Data Resources

Tech Data Security Solutions Hub

http://www.techdata.com/techsolutions/security/

Tech Data's Security Solutions cover endpoint to endpoint and all points in between. We've closed the loop on security technologies and provide you with the tools and services you need to make your security business the most profitable.

TDCloud

http://www.techdata.com/content/tdcloud/default.aspx

TDCloud is a set of products, services and enablement tools available from Tech Data that help VAR customers find, develop and close Cloud opportunities.

TDAgency

www.techdata.com/tdagency

TDAgency is Tech Data's full-service advertising and marketing agency and we have something other agencies don't have—IT industry experience and expertise. Why waste time explaining your solutions to someone who doesn't live and breathe IT? We can hit the ground running and work with you to develop a targeted strategy and customized marketing plan for resellers of all sizes and budgets.

MyLicense Tracker

http://www.techdata.com/tools/licensing/LicenseResendSearch.aspx

This automated search enables you to search for and forward license e-mails for select vendors.

Software License Selector Powered by StreamOne [SM]

http://www.techdata.com/TDSKUSelector.aspx

Tech Data's Software License Selector powered by StreamOne[SM] significantly surpasses contemporary software licensing tools in breadth and ease-of-use. It supports 40 major software vendors, representing more than 99 percent of the software licenses sold through Tech Data. It eliminates the need for you to spend valuable time researching each vendor's unique and often complex software licensing programs, because Tech Data has done all the work for you.