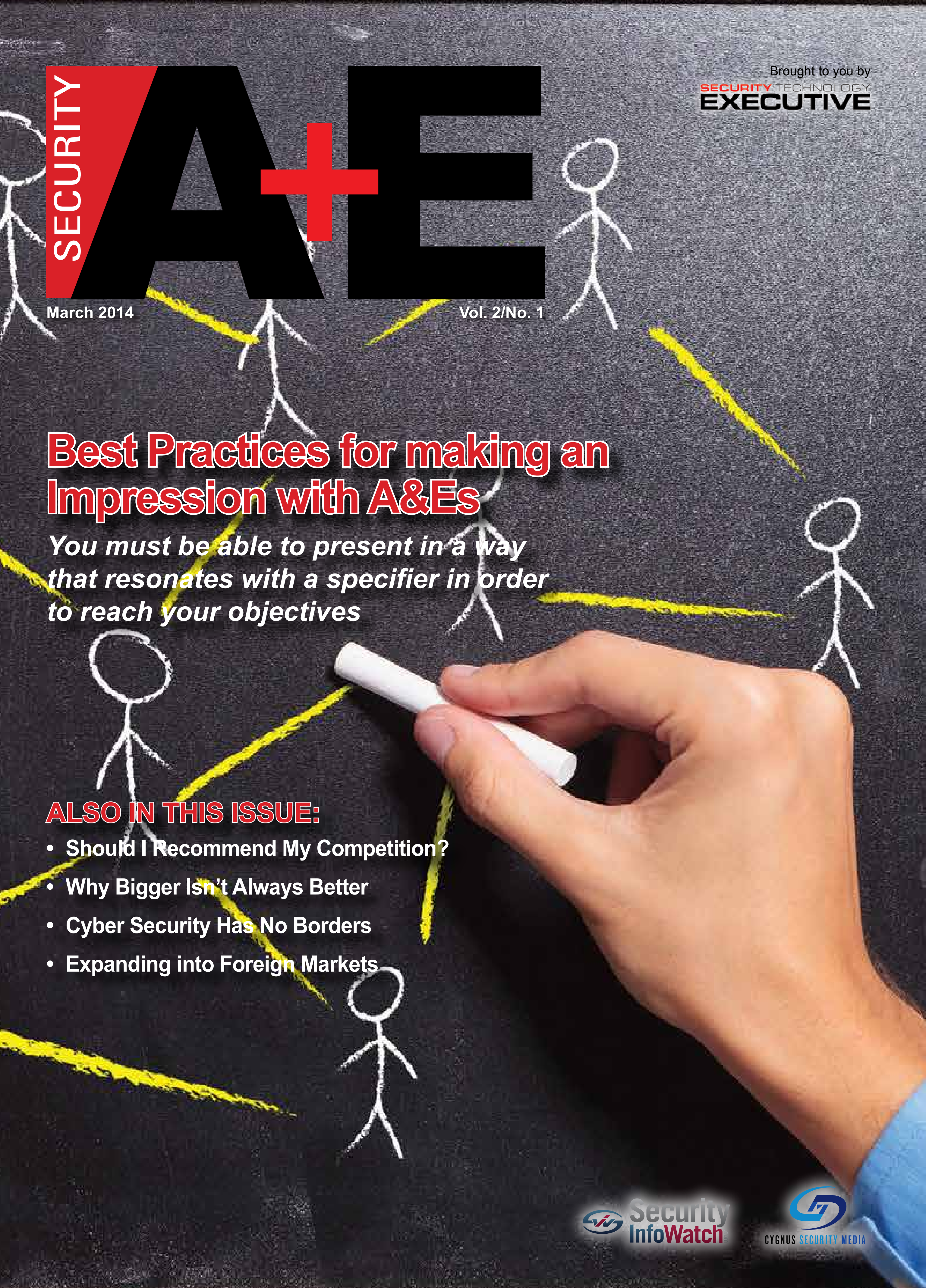
Brought to you by
SECURITY TECHNOLOGY EXECUTIVE

SECURITY A+E

March 2014 Vol. 2/No. 1



Best Practices for making an Impression with A&Es

You must be able to present in a way that resonates with a specifier in order to reach your objectives

ALSO IN THIS ISSUE:

- Should I Recommend My Competition?
- Why Bigger Isn't Always Better
- Cyber Security Has No Borders
- Expanding into Foreign Markets

Security InfoWatch
CYGNUS SECURITY MEDIA

By Steve Lasky, *Editorial Director of Cygnus Security Media*

Every consultant needs some skin in the game

Most of us describe it as a work in progress. That ever expanding circle of trust we call the security consultant and vendor relationship.

The fact that the lines of communication are sometimes garbled between the two worlds presents a problem that eventually affects the client. Over the past several years we have seen many technology vendors who have been diligent in their efforts to embrace relationships with industry consultants. There is not only room for improvement, but a critical need to have this happen.

As technology morphs from analog to digital and services rise from buried cables to the cloud, a cohesive partnership will ensure consultants have skin in the game. Talking to several top industry consultants, the consensus seems to reflect a roadmap of cooperation.

One consultant tells me that the key to this enhanced relationship is that vendors have developed a better understanding what consultants do and are providing resources to help them serve their clients more effectively. “There is seldom a week that goes by that a manufacturer has not asked for an opportunity to stop by our office to bring us up to date on their technology and often times their product development roadmap,” says this consultant.

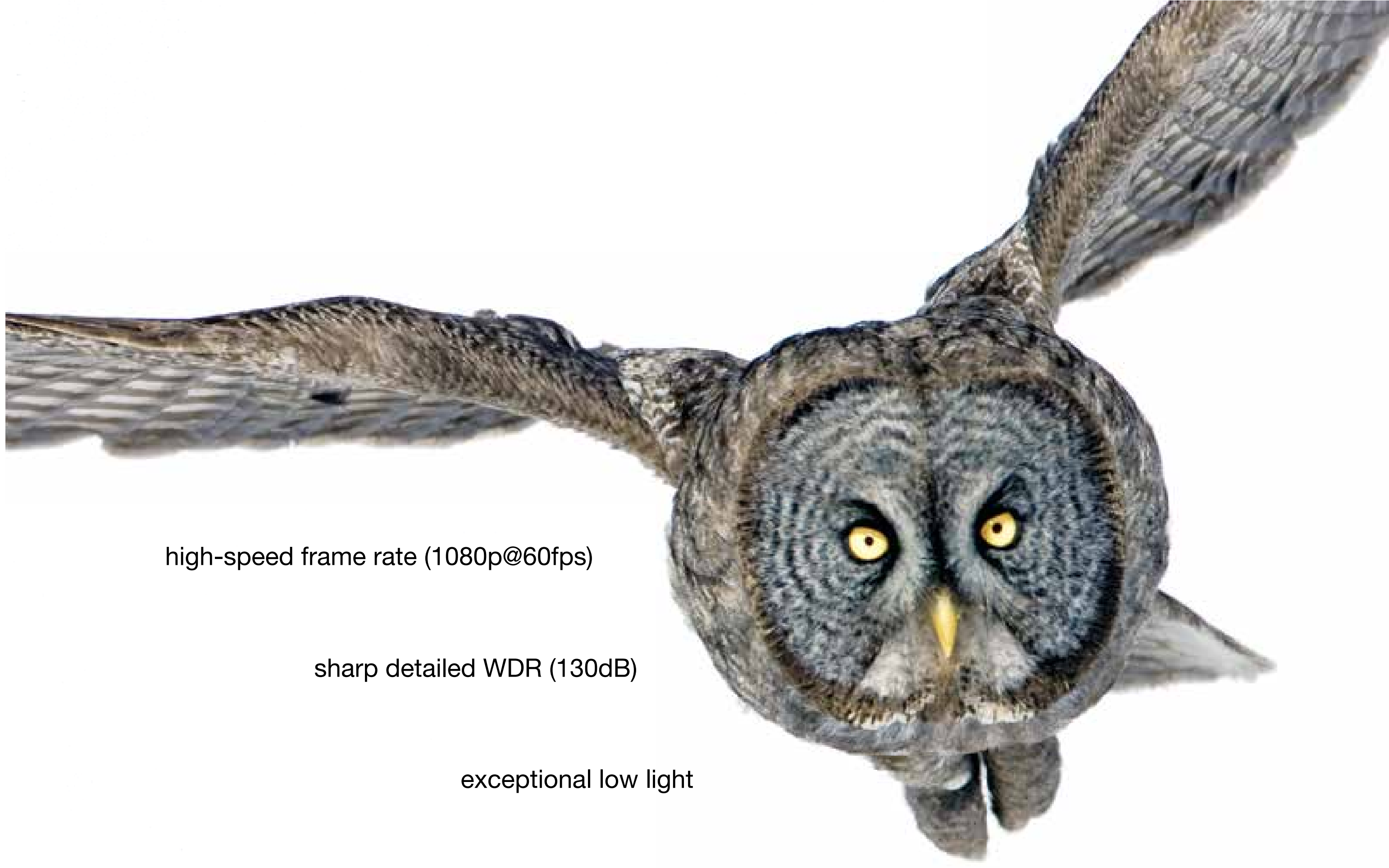
While another consultant admits that some manufactures do this better than others, he appreciates the effort. “Sometimes these update visits almost become a sales call. We discourage that. What we are looking for is an interactive discussion about the technologies and their applications and what the manufacturer is doing to support their integrators and end users.“he says.

Collaborative relationships can result in vendors taking a number of new product enhancements to R&D.

As more and more manufacturers make their web sites A&E-friendly, providing access for updated specifications, data sheets, and even three dimensional drawings, everyone in the industry wins.

SECURITY A+E

MARCH 2014



high-speed frame rate (1080p@60fps)
sharp detailed WDR (130dB)
exceptional low light

By Chris Peterson, *President, Vector Firm*

Top 10 best practices in presenting to architects, engineers and consultants

You must be able to present in way that resonates with a specifier in order to reach your objectives

Presenting to an audience is the most powerful action taken by a sales professional. Regardless of the dozens of communication methods at our fingertips today, public speaking is still the most influential mode of transferring emotion. The problem is that most professionals today are poor presenters.

In the security industry, presenting to a specifier is a skill that can separate one company from their competitors -- if done correctly. The objective of pursuing relationships with architects, engineers and consultants is to have your products specified into more projects. In order to achieve your objective, you must be able to present in a way that resonates with the specifier. Below are 10 best practices for presenting to specifiers in the security industry. (For this article, I've given the best practices for presenting to specifiers as a whole rather than break it down to architects, engineers, and consultants.)

1. Customize your presentation for the specifier. I'm amazed how many sales people give the same presentation to an A&E firm as they give to an end-user or VAR. This audience is completely different in need, interest, and personality. However, many times the old PowerPoint that was just given to a facilities manager at a university is shined up on the screen in front of a half dozen people who will never use the product but might need it as part of a larger design.

2. Don't make your presentation over-the-top in technical jargon. A common mistake made by good sales people with great intentions is to take the sales presentation and make it super techy for the "smart guys". It doesn't matter how intelligent your audience is, reading data off of a chart will put them to sleep. Even though this audience has different needs than an end-user, they still need to hear entertaining stories in an organized and logical order to hold their attention. Don't bore them with your really cool words and graphs.

3. Send a glossary of special terms and other helpful material ahead of time. Designing security projects requires a broad knowledge of many technologies. Being up to date on the special terms from all the different technologies is almost impossible. Develop a glossary of terms for your technology and email it (and any other helpful material) to the audience a few days before your presentation. I once observed a thermal imaging sales person present to a consultant with a strong video background. Unfortunately, his experience was minimal in thermal imaging and he wasn't familiar with some of the terms unique to the technology. A simple glossary would have solved this problem and kept the presentation very fluid. Also, consider how professional this small gesture makes you appear.

4. Share the good and the bad about your offering. If your product was perfect for all applications, your company wouldn't need you to help sell it. Prepare a list of your product's limitations and invite a candid conversation with the audience about these weaknesses. Don't celebrate your weaknesses, but be honest and confident about them. Explain where this affects the product's performance and where it doesn't really matter. This will help the specifier develop an area where your product can be ideally positioned, and will place you at the top of the list of credible sales professionals.

5. Share real stories and examples. There is nothing better for retaining attention of an audience than telling a story that is emotionally relevant. Have fun and make fun of yourself. Don't just tell them about the wide temperature range that your widget can handle; tell them a story about the demo you did in Chicago last January when your watch stopped but your widget kept working -- but you missed your flight because of your watch. Tell stories that are true and relevant, and your audience will love you for it. Stories will help your audience remember you months in the future when they might need to specify your product.

6. Don't get caught up in discussing technical detail during the presentation. I think it's a universal requirement: every presentation has to have that guy in the back who wants to show everyone how smart he is by dragging you into the weeds of technical details. Don't let it happen. There are many techniques to overcoming this trap, but the best thing you can do is acknowledge and promise. Be prepared with material to distribute after the presentation, acknowledge the question with appreciation, and promise that the material you'll give them after the presentation will answer all the technical questions. Finally, let the smart guy in the back know that you're happy to discuss this with him in detail after the presentation. No matter how technical the audience, once you fall into this trap, you've lost them (except the guy in the back of the room).

7. Discuss your sales and support process. It's not all about your product. If you do not support their client, it reflects very poorly on the specifier. Toward the end of the presentation, discuss your sales model and your post-sales support process. How do you support your reseller, what is your warranty, how do you handle version control and compatibility? Tell a story about your product failing and how your company handled it by following your process. Don't talk about how "customer-centric" you are or how service is the number one priority in your company – everyone at every company in every industry states this. Discuss the written policy and tell them a story about how it has been practiced.

8. Let the audience know how to work with your company. All of us like to think that our products are so cool that the specifiers will break through walls to work with us. However, if it's not fairly easy to work with your company, they'll find someone comparable. During your presentation, show them the multiple ways to work with you and take it a step further. Call the 800 number where a live person answers, call up your website and show them the specifier section where all the drawings, pricing, and specifications can be found, and make sure they all have your contact information.

9. If appropriate, bring demo equipment and samples. Retention of information is directly related to the number of senses that are stimulated. If you can bring something to touch, feel, and see, the audience will remember you in much more detail than your competitor that runs through a PowerPoint.

10. During the presentation, establish a protocol of ongoing education. One lunch and learn won't do it. If you want

> *"In the security industry, presenting to a specifier is a skill that can separate one company from their competitors — if done correctly. The objective of pursuing relationships with architects, engineers and consultants is to have your products specified into more projects."*

> *"A common mistake made by good sales people with great intentions is to take the sales presentation and make it super techy for the 'smart guys'".*

to make an impact in the world of architects, engineers and consultants, you'll have to bring them value on a consistent basis… and this doesn't mean the same presentation over and over again. As you're wrapping up your next presentation with a specifier, let them know that you'll be bringing valuable information a few times per year. Ask them for ideas for topics and for the best way to schedule these meetings. It will end your presentation with a feeling of a continued relationship rather than the ending to a meeting.

Implementing these best practices will require extra effort and possible resistance from your organization. However, there is no better method of winning business than being specified into a project. Working with architects, engineers and consultants will help position you for success, but regularly presenting to them in a tailored, entertaining, and informative manner will completely separate you from your competitors. Regardless of the hard work and internal pushback, press forward and implement these 10 best practices. I promise the rewards will be worth it.

About the author: *Chris Peterson has nearly 20 years of experience in sales leadership, with a focus on creating strategic sales processes. Before embarking on a career in sales process consulting, Mr. Peterson developed a philosophy of repeatability and refinement for the sales professional. He has become an expert in customizing CRM methodologies and systems to optimize the efficiency and effectiveness of today's sales professional. Combining technology and an understanding of the sales and customer service personalities, Mr. Peterson has been able to implement programs that are fully utilized by the client-facing teams and management, with a result of improved efficiency, higher closing ratios, and reduced customer attrition.*

Mr. Peterson has created sales processes in many industries, including aerospace, automotive, defense, healthcare, IT, security, and telecommunications. Mr. Peterson can be reached at cpeterson@vectorfirm.com.

By Ray Coulombe, *founder and managing director of SecuritySpecifiers.com*

Should I Recommend My Competition?

For a manufacturer, an A&E program is a commitment to the future

Too often, people sell what they have instead of focusing on solving the customer or client problem. It takes moxie to step out of the box and, if necessary, recommend a competitor's solution. For a manufacturer, an A&E program is a commitment to the future, and a short term 'hit' can yield big long term benefits.

Let's start at the beginning. What's the real purpose of an A&E program for manufacturers? The expected answer is to get products specified. But, if given the choice between the following expanded answers, which would you pick?

A. Get products specified on a current project

B. Get products regularly specified

Answer A is winning the battle. Answer B is winning the war.

Winning the war requires building a serious long-term trusted relationship with a security consultant or engineer. Just as good friendships and marriages take time, hard work, and addressing problems head on, that same commitment is a must for establishing long term consultant relationships. Solid relationships are bi-directional and need a spirit of commitment on the part of each partner to make them work.

A consultant's time is valuable, but some of that time should be allocated to understanding the product and technology solutions available to them, in addition to applying those solutions in a project environment. One representing a security product should be sensitive to the consultant's time and needs by consistently delivering the goods -- timely, accurate product and application information.

Making the design phase work

In the design phase, a product rep should make sure that the consulting firm has a full product "care package" that includes:

- Properly formatted specifications
- Current data sheets, with specifications consistent across related documents
- Operation and installation manuals
- Design guides
- Applicable reference standards and codes
- CAD libraries
- BIM libraries
- Training videos
- Technology tutorials

In the old days, much of this would be resident in a three-ring binder sitting in a conference room or hallway bookcase. Today, however, companies should be focused on myriad vendor web portals providing access to totally up-to-date information.

The Construction Specification Institute (CSI) recently published its Practice Guide for Construction Product Representation. Its Task Items cover the following areas spanning several project stages:

- Meet with designer/design team; learn and understand project design intent.
- Determine project's product/system/material needs.
- Recommend product/system solutions/applications to meet project requirements.
- Provide timely and accurate responses to product selection questions.
- Provide/edit specification sections for project specific products/systems/materials.
- Provide drawings and calculations to address project requirements.
- Provide budget pricing.
- Suggest ancillary products compatible with specified products/systems/materials.
- Estimate product/system/material lead-time.
- Identify codes, rules, regulations, and jurisdictional requirements applicable to the product/system/material.

Provide product/system/material storage, handling, installation, and maintenance requirements.

- Provide and interpret applicable product/system/material warranties
- Inform customers of proper and improper applications for product/system
- Communicate identified market trends to product/system manufacturer
- Nurturing the consultant and product rep relationship

All of the above action items suggest that the Product Representative can be a valuable member of the project team; a position achieved through helpful actions and not hollow sales promises. A good product rep

- knows his product
- knows his completion
- understands his company's roadmap
- has management's confidence
- gets answers in a timely fashion
- tells the truth

Good representatives provide this. Good consultants demand it.

So, let's envision a scenario where a consultant has been provided by a large client with an unusual set of circumstances that demand some very specific product features. As it so happens, his favorite product rep is due in for a meeting that day. The consultant relates his need, and the rep realizes that not only does he not have a product with the required features, but a key competitor does. What are his choices?

Fib - Tell the consultant that the product can do the job. This is really a problem if the representative has no idea what his products can do. Unfortunately, this happens too often, and lack of product knowledge benefits neither party. Message to manufacturers: train your people on product and conduct.

Fib - Tell the consultant it's coming out next quarter. Manufacturers must provide accurate product roadmaps to their representatives to avoid overcommitting to a schedule. Conversely, reps must bring feedback back to their manufacturers on schedule and emerging technical requirements as critical inputs to roadmap planning.

Fib - Say nothing like that exists nor

> *"A consultant's time is valuable, but some of that time should be allocated to understanding the product and technology solutions available to them, in addition to applying those solutions in a project environment."*

is likely to exist. Product reps must understand the current technology and competitive landscapes. This requires not only manufacturer training, but also personal diligence and study. What is the current state of the art in technology? Where does my product fit? How will these evolve over time? Discussing these issues with consultants and getting their perspectives can lead to fruitful discussions, mutual respect, and areas for further investigation.

Stall - Commit to get something designed in time for the project. This is easier said than done, since few reps can commit to a project on their own. Bringing in one with the authority to commit or getting it on the company agenda for product discussions are feasible, and may lead to a viable approach that will address the current need. Also, valuable new products may emerge from the dialog.

Engineer - Review the project requirements to determine possible alternative solutions. Rarely is there only solution to a security project requirement. If consultant ego is not a factor, the rep can play a valuable role by listening and really understanding the nature of the requirement. Through his knowledge, experience, research, and company resources, he should attempt to put alternative solutions on the table for discussion.

Engineer - Persuade his company to develop and meet the technical and schedule requirements of the project. Generally, this will only happen if the technical hurdles are modest, resources are available to address them, and the product rep has enough internal credibility to stimulate action. It may also occur if someone has made a strategic judgment that the company must participate in the project for competitive position, prestige, marketing, or future business reasons.

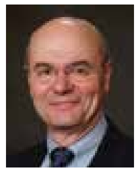
Partner - Convince his company to collaborate with a third party to license, private label, or technically cooperate to present a viable solution. In today's world of API's, standard interfaces, and protocols, it might be possible to append a capability to a product that delivers a solution. Engineering resources are still required and companies with strong partner programs are in the best position to pursue this avenue.

Recommend - Point out competitive products that meet the consultant's need. Let's digress to the title of this article. This takes guts (or stupidity, depending on your point of view) and isn't likely to happen very often. And a product representative probably wouldn't tell management if he went this route. However, this could be great way to build trust and confidence, not to mention taking a giant step in the relationship's development. And what has really been lost? The company's product has not been unknowingly mis-specified or misapplied. Promised time schedules won't be broken, the company avoids an opportunity to fail, and the opportunity may come back around in another way.

On the consultant's part, when a product rep takes the riskier higher path, his behavior should be recognized and valued. Most consultants have been burned by "slick sales" behavior in the past and may be skeptical of a manufacturer's claims that something is just around the corner or will soon be in production, ready to roll in time to support the project.

However, successful consultants recognize and value when a rep is truly trying to do the right thing. Rewarding his honesty and good intention by placing him in the role of a trusted advisor encourages the right kind of behavior and enables a potentially valuable resource. This is enhanced even further if the company he represents has a track record of successful projects and products that work; useful literature and design information and tools; design support; strong integrator partners; and a collaborative attitude.

That's a company and a representative you can work with.



About the author: *Ray Coulombe is Founder and Managing Director of SecuritySpecifiers.com and RepsForSecurity.com, and Principal Consultant for Gilwell Technology Services. Ray can be reached at ray@SecuritySpecifiers.com through LinkedIn at www.linkedin.com/in/raycoulombe or followed on Twitter@RayCoulombe.*

By Robert Laughlin, president, Galaxy Control Systems

Why bigger isn't always better when selecting an access control partner

Smaller vendors can be more flexible and open to customization for their customers

Note: Galaxy Control Systems President Robert Laughlin offers a personal view related to his experiences of the advantages of working with small to mid-sized access control technology vendors based on his many years as one of the industry's most respected technology pioneers.

We've seen an increase in the number of conglomerates formed in the security industry over the past several years. Conversely, we've seen some conglomerates dissolved and broken back down into individual and often privately held companies. Needless to say it's an interesting cycle, especially from the perspective of an independent access control company playing in the same market .

At the end of the day though, one needs to look at the business ramifications that customers face when dealing with big versus small to medium sized technology providers. Given the nature of access control systems and the on-going service and support these systems demand to ensure continuous and reliable operation, small to medium size access control partners can often deliver more advantages given their technology focus and customer relations. Here's some food for thought.

Innovation is big at small companies

Every facility and installation is different. Even franchised businesses that follow the same construction and design models are never quite the same from one to the next. Consequently, off-the-shelf access control solutions rarely provide the specific versatility and desired functionality that customers are looking for in their particular situation. It's no secret that some big companies have problems dealing with anything that could be conceived as "customized" and typically leave that task to the installing dealer or customer's internal techies.

Small/medium access control solution providers have built their businesses on catering to the specific needs of customers and their installations of all sizes and geographies. The same holds true in terms of software development. Competing against big companies' marketing budgets and sophisticated sales pitches requires small/medium technology providers to be innovative in terms of developing new solutions, while at the same time being conscious of a customer's investment in existing legacy technologies. Providing new solutions to longstanding problems that can be implemented on legacy and future access control system deployments is innovative. Rip and replacement solutions are not.

Making personal connections

It's interesting to note that some big companies frequently invest big dollars trying to emulate the intimate relationships that small companies establish with their customers. And the focus on customer service is a trending issue which continues to be well represented in social media with big and small brands alike. Most small/medium sized independent companies don't need to work on building personal relationships with their reseller partners and customers as they are typically built this way from the start. The fact is that all customers want to feel as if they are your most important customer – and that you intimately understand their needs and connect to them.

Communicating clearly and with substance

In this day of instantaneous and constant communications, why is it that personal connections sometimes seem more difficult than ever before? Perhaps it's the reluctance of today's workers to pick up the telephone and actually speak with customers, or the fact that individuals are more tasked than they were in prior years with a relentless assault of communications 24/7/365.

This seems to be more the case with the larger companies, as the number of internal interactions at a large company typically increases to reply to important issues. Many smaller companies are modeled to be more streamlined and can react faster to questions and issues simply because they are not as layered. The people who sold the system are typically accountable for supporting their customers and can spend more time communicating electronically, over the phone or in person. At the end of the day, customers want to know that they have a go-to person they can rely on when they need them most – which typically is when something goes wrong. Small/medium companies generally deliver clearer and more direct lines of communication, which expedites information sharing.

Making timely decisions

Decision-making processes in smaller organizations are often dramatically different from those in their larger counterparts. Big organizations are typically layered with varying levels of specialists to cover basic support functions. This may delay important decisions since the personnel authorized to resolve important issues need time to collect data and review it before taking action. Dealing with committees in a bureaucracy slows down progress. Small/medium size businesses tend to react faster as employees know their customers and their systems better, and have shorter reporting paths to decision makers.

Small/medium business attract team members

One of the inherent complaints individuals make about working in large companies is that they may get lost in the machinery of big business environments. Small/medium sized businesses attract people who thrive in environments where they feel like they are part of a team. And that's great for customer relations, especially in technical areas where the intricacies of a system make all the difference in terms of service and support. This not only boosts customer confidence, it helps further develop longstanding relationships, and helping customers keep their systems running smoothly.

(continued on page 26)

By Dr. Armelle Fée

Expanding into foreign markets requires a total understanding of the environment

If localization is not well-planed it will lead to frustration among your employees and customers

“The limits of my language mean the limits of my world.” -- Austrian-British philosopher, Ludwig Wittgenstein (1889-1951)

In our ever-broadening world, limits often are an impediment to growth. I have stated the obvious. But how can you go about growing your business in this big, wide, ever expanding world? One of the many answers is “localization”.

You have heard this word; you know it has to do with translating your products into other languages. You know that translated products will increase your presence worldwide, augment your sales and enhance customer satisfaction. However, having heard about well-known localization disasters (such as the infamous Nova car marketed for a Spanish-speaking client that really would rather not buy a “no-go” car), you might feel a little apprehensive about going beyond the limits of your world, your language. You know that if localization is not well-planed it will lead to frustration among your employees and customers, cost you more money and headaches than needed and could really jeopardize the in-country integrity of your brand.

Before embarking on such a rewarding journey, it is best to understand what translation, localization and all these “-ation” words mean, who the key players are and the processes that will take your products there. This is the first installment in a series aimed at giving you an understanding of the voyage so you can embark on it confidently, leading your team to success.

So what is localization?

Let’s start with defining these “-ation” words! What is localization? In essence, localization is the process of adapting your product or the services you offer to a specific language and to the cultures utilizing this language so you achieve a local look-and-feel. Often abbreviated as L10n (l for the first letter; n for the last one; and 10 for the 10 letters contained between the l and the n), localization is best implemented after proper internationalization (also known as I18n; and yes, you got it, you know what this means).

Internationalization, in the software industry, is the process of designing a software application in such ways that it can be adapted to various languages and regions without having to make further engineering changes. And for items such as documentation, think of it in terms of writing for localization, which we will discuss in more detail in a future article. Then, there is globalization (abbreviated as… G –giving you time to count… Alright! G11n, you’re good!!!), which is simply about leveraging a thing to several different countries.

Now, let me throw in another “-ation”, one you are most likely familiar with: “translation”. This one is easy and the Merriam-Webster definition is perfect: “a rendering from one language into another”. A partner to localization is “pseudo-translation” (also called “pseudo-localization”). This process is a software testing method used for testing the various internationalization aspects of software. Let’s round out the “-ation” family with Translation memory (abbreviated as… T… Are you thinking T15y? Nope, it would not follow the Letter-number-n pattern; it is simply TM). Throughout the localization project and after (and here we would be talking about translation memory management), a TM helps capture and store “segments”, which can be sentences, paragraphs or

sentence-like units, in a database in order to assist human translators.

Another term to define as it pertains to the process is “Quality Assurance”. In our context, Quality Assurance (a process which involves several key steps) can be defined as testing of the translated files to ensure they function as intended and checking the translation during linguistic and terminology reviews.

How to make the process work

When embarking on a localization project, it is essential that you surround yourself with a team that will work with localization in mind. All on board will have to play their part knowing that what they create or do will need to flow as effortlessly as possible throughout the process. We will touch on the process, but first, let’s take a look at the key players that will form your winning team.

I like to place them in five categories: content writers, translators, quality assurance engineers, reviewers and project managers. Content writers, such as software developers, technical publication writers and marketing writers, will need to write in such ways as to facilitate the upcoming translation of the content they will deliver. In a separate issue we will look at the many guidelines that ensure the translatability of content; but for now, suffice to say that if your content is designed as an afterthought to localization, you are more than likely to experience various challenges that are likely to have a negative impact on quality, time to market and budget.

> “Before embarking on such a rewarding journey, it is best to understand what translation, localization and all these ‘-ation’ words mean, who the key players are and the processes that will take your products there.”

The Language Service Provider (LSP) you will partner with will mainly ensure the quality of the translations, although their involvement may be greater. The relationship you will develop with this team is paramount to the initial and continued success of your project. Your in-house quality assurance team will also play a crucial role in determining the readiness of your product for your intended market(s). The reviewer of the translated content will verify that the translator has applied your requirements and produced a quality translation. You may look at these four main players as puzzle pieces that your project manager will ensure are put together to fit perfectly for the right picture to appear. Some in the industry may argue that project management would lie on your LSP’s side, but I am a firm advocate of having someone in-house manage the localization project. This manager’s involvement may vary depending on the complexity of the tasks at hand, but his or her role is essential: mainly, ensure quality, adherence to budget and deadlines.

Content is king

Onto the last topic I would like to familiarize you with in this first article of the series: process. Processes are ultimately unique to your needs, but there are general threads that apply to just about any project. First and foremost, write with localization in mind. In future articles, we will look more closely at what one needs to do so that the content is easier to translate (which usually means cheaper, too).

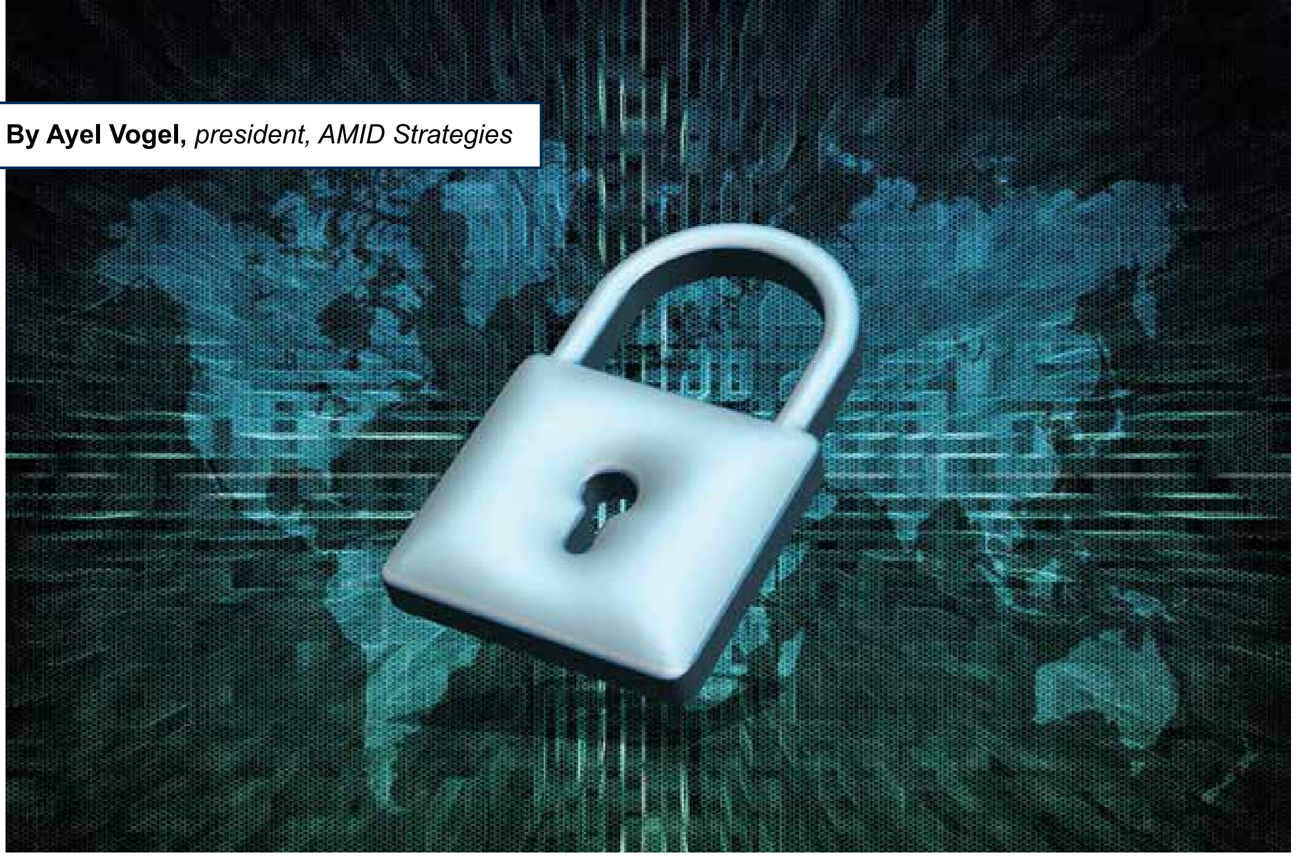
But let us just say for now that this means that when the content is created, remember that someone will translate it and your content will go through many hands and be seen by many eyes. A general process that could apply to just about any kind of content, be it software, user guides, marketing documents, web sites, looks like this:

1. Content is written and a glossary is developed in parallel
2. Pseudo-localization takes place (this is particularly relevant in the software field)
3. Content is exported for quotation
4. Translation takes place
5. Review follows (and we will see this review entails several steps and takes several forms depending on the type of content being verified)
6. Changes are implemented as needed (ideally, you would have steps 4, 5 and 6 completed for the glossary and then performed for the content itself); and finally
7. Release your localized product and harvest the fruits of your team’s hard work! Wait, one last thing to keep in mind, and this may have needed to start already somewhere along the aforementioned process: get ready for the next version!

If you were not familiar with localization, I hope that these few words have given you a general understanding of what your localization journey might look like. Localization is fun, really! Well, I love it, I am passionate about it, and I love working with all involved in this process because it is such a rewarding feeling to see my clients reach their globalization goals! The world is waiting for you. Surround yourself with the right team and go out there and win it!

About the author: *Dr. Armelle Fée is a multi-lingual localization professional with 20 years of experience, including 14 in the security industry. Educated in both France and the U.S., she has lived and traveled around the world, and has a sharp understanding of doing business in a foreign environment. Should you have questions or need a little help with readying your product for the market, or various markets you intend to offer your services and products to, feel free to contact her at armellefee@netzero.com.*

By Ayel Vogel, *president, AMID Strategies*



Cyber security has no borders

A sound cyber security strategy is no longer optional, but an imperative foundation for any organization

In the broadest term, cyber security is defined as the method of protecting a computer system, including all networks and connected devices, from illegal intrusion and malicious activity, as well as from human error and natural disasters.

In practice, we need to assume that every computer network component in every organization may be a target for intrusion and cyber-crime. A cyber-attack can be devastating to the organization and its customers. An attack can take the form of stolen financial information, industrial espionage, politically- or financially-driven denial-of-service (DoS/DDoS) attacks and damages to SCADA-controlled manufacturing processes or infrastructure facilities, as well as a variety of ransom-ware, malware and other worms and viruses. In addition, an attack can open up a company to lawsuits from customers, partners and other parties.

The severity and complexity of cyber security make it impossible to specify a simple solution. There is no "magic-bullet" software or firewall that can protect an organization from all cyber attacks; moreover, a balance needs to be maintained between securing operations and allowing the organization to function smoothly.

What is needed, then, is a comprehensive cyber security strategy/methodology, which prescribes an ongoing risk assessment, awareness of the newest security tools and technology trends, and implementation of procedures. All of these must be integrated with the physical security system (to protect against cyber-threats involving physical intrusion).

This is where security consultants and experts come in.

I'd like to make this point crystal clear: serious cyber security requires very specific expertise, the kind that most IT managers do not possess. You need to hire a consultant with experience in your (or very similar) industry, who will work with your IT manager (or the A&E consultant at a project's inception stage).

"You hardly ever hear a customer say, 'We don't know what we don't know.' That's the right attitude, because in fact, they don't know what they need," said Joseph Baker, partner at Atriade, a Jersey City, N.J.-based professional technology consulting firm. In an ideal world, he said, "customers would ask you to hack into their systems and expose vulnerabilities, but in most cases, all they ask for is compliance with whichever regulations apply to them."

In addition, since the organization has different stakeholders, each protecting their own interests, an executive (usually the CSO) needs to be involved at the highest level to fully understand the security risks and integrate a collaborative strategy that would bring all the stakeholders together.

For example, the stakeholders for a cyber security implementation in a typical electric utility include the network/IT manager, the physical security manager and the ICS (industrial control systems) person. The goal of the CSO, working with the cyber security consultant, is to identify a single, unified solution that meets the requirements—and protects the interests—of all three stakeholders, rather than providing disparate solutions for network intrusion, integration with the physical security system and detection of malicious behaviors in the ICS system.

In general, cyber security can be broken down to a number of intertwined elements:

• User Authorization – the compartmentalization of information that defines who can access which information, under which circumstances and conditions. This element includes the authorization software as well as the protocols and procedures for accessing data.

• Intrusion Detection and Prevention Systems (IDS/IPS) – appliances placed on the corporate network that monitor network traffic to identify, log, block and report malicious activity.

• Device Protection – software tools that reside on network-connected devices to detect viruses and other malware.

• Network Separation and Secure Data Switching - separation between different functional

networks and securing inter-network connections.

• Encryption – both stored data and data communication need to be adequately encrypted. Remember, however, that data encryption is the last defense against cyber threats, since no data should ever been have exposed to intruders from the start.

These elements are not optional or interchangeable—each and every one needs to be set in place to assure the proper protection of data and data traffic.

> *"The CSO's job is to evaluate the repercussions of each and every addition to the system, and ensure that every device is connected to a secure switch designed to detect and block any unusual network behavior."*

Sometimes, vulnerabilities are piled onto an initially secure computer network through expansions and added functionality. For example, many municipalities in recent years have implemented "Safe City" practices, with hundreds or even thousands of cameras canvassing the city center, roads and public buildings. The camera, recording server and operator networks use standard switches for automation and communication, creating a huge security threat at the gateways to the municipal network. This makes each camera location a potential point of intrusion into the network. The CSO's job is to evaluate the repercussions of each and every addition to the system, and ensure that every device is connected to a secure switch designed to detect and block any unusual network behavior.

I've observed many cases where there is over-reliance on securing the network perimeter —incoming and outgoing data, as well as on encryption—while neglecting two major vulnerabilities: lax protocols for data access and inter-network switching.

"The weakest link in cyber security today is corporations' social engineering," said Thomas L. Norman, CPP/PSP/CSC, CEO at Protection Partners International, and author of "Integrated Security Systems Design: Concepts, Specifications, and Implementation" (Butterworth-Heinemann, 2007). He noted that the best cyber security scheme is worthless if, for example, passwords are stored unencrypted in plain text on an employee's laptop that can be stolen; if the server room is not adequately protected; or if security cameras' login passwords are not changed routinely (or at all). All of these are real-life occurrences.

To illustrate his point, Norman brings the example of the current CyberLocker virus which has to date infected a quarter of a million computers around the world. Once infected, and unless ransom was paid in Bitcoin, the virus encrypts and disables the entire network – SAN, attached storage, internal, workstations. What's even more shocking, the virus propagates through email, exploiting employees' reluctance to comply with the most basic rule of online behavior.

Another example is the recent cyber-attack on Target and two other major retailers, which compromised over 40 million credit cards. The attack allegedly involved obtaining access authorization from the data center's HVAC vendor (probably by calling the vendor and impersonating an IT department official.) "Intrusion used to mean entering a facility through a manhole -- today's manholes can be in Eastern Europe or anywhere in the world," he warned. "You have to have each and every base covered."

The Target attack also reveals another commonplace vulnerability: insecure inter-network switches. In the Target case, according to Norman, "even if the hackers were able to enter the HVAC network, and wreaked havoc there, they shouldn't have been able to access customers' credit card data." Exacerbating the problem is the fact that U.S. credit card issuers have yet to adapt "smart" credit cards, which greatly reduce credit card fraud.

As I mentioned, inter-network switching protection is a common vulnerability in many corporate IP environments. The larger, more complex and more geographically distributed the network, the more it is susceptible to hacking—and nowhere is the danger more apparent than in infrastructure, utility and power generation installations. These large-scale distributed systems often involve dozens of critical facilities across multiple states. In the case of failure the potential for damage is immense, as recently demonstrated by the Stuxnet attack, which caused uranium-enrichment centrifuges in Iran to self-destruct.

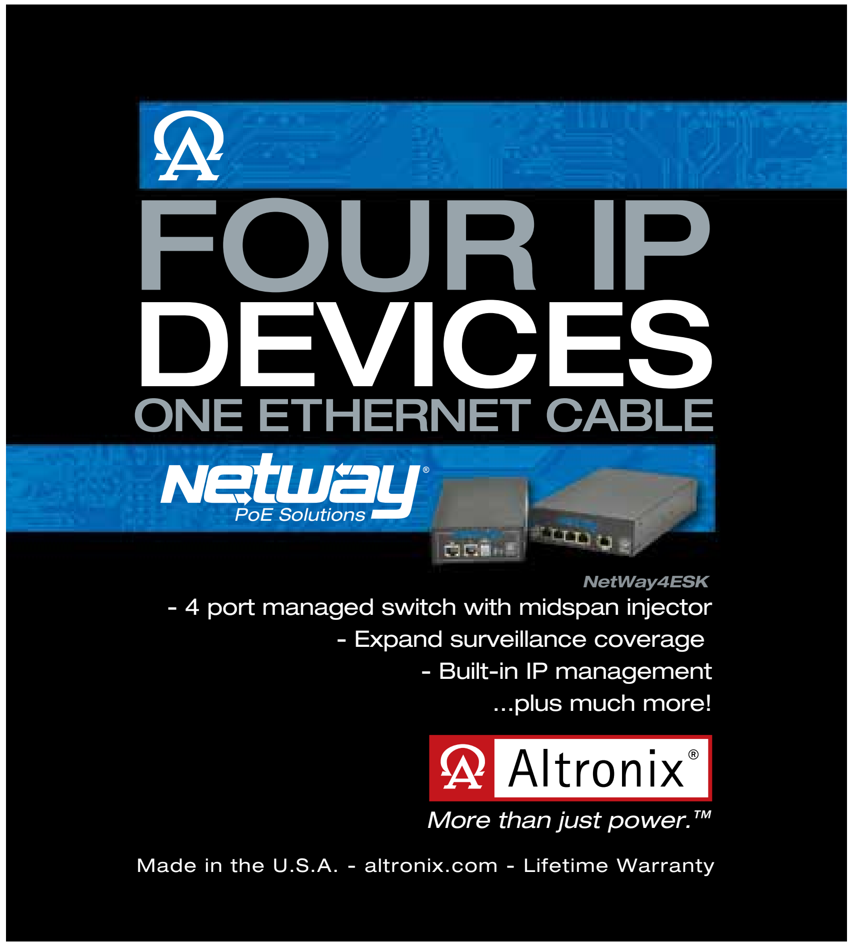
Most such installations employ SCADA (supervisory control and data acquisition) industrial control systems (ICS), computer-controlled systems for monitoring and controlling industrial processes. However, SCADA systems pose a unique cyber security challenge. Joseph Baker explained: "SCADA is an antiquated, serial-based protocol for automating and collecting data in closed-environment industrial control systems. It had no security designed in from the onset—and yet is it used to run the most critical applications."

As such, there are very few intrinsic approaches to secure SCADA. In fact, the best strategies are to make critical infrastructure networks disappear by becoming invisible to hackers, and to closely protect inter-network data switching for untypical behaviors.

"The greatest challenge in the event of a cyber-attack is to contain the propagation of the threat from one site to another through the internal network," said Ilan Barda, CEO of RADiFlow Ltd., which manufactures secure industrial ethernet solutions for critical infrastructure SCADA applications. "This is due to the operational interdependency between sites. For example, an electricity grid that is dependent on sharing production between different sites, to prevent overloading the generator turbines at a single site."

Isolating a threat within an internal network is done by placing "smart switches" at each site or internal network. These switches, which double as communication gateways and a SCADA-specific high-throughput IPS (Intrusion Prevention) solution, analyze the behavior of the incoming SCADA protocols (adjusted to a set baseline), and are able to immediately react upon identifying stray behaviors, which are in turn logged and reported.

Unfortunately, I can't emphasize enough that when it comes to cyber



security, many critical infrastructure networks in the U.S. are still far from airtight.

Looking ahead, an important driving force behind stronger data protection is the advent of new standards, which provide a roadmap for setting up cyber security mechanisms and protocols. These include the NIST Security Framework, created by executive order of the Obama administration and finalized in February 2014, aimed at "addressing and managing cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses" (www.nist.gov/cyberframework/); NERC (North American Electric Reliability Corporation) cyber security standards, relevant to the electricity generation and transport industries (www.nerc.com); and the ISO/IEC 27000 series of non-binding standards for different infrastructure verticals, among others.

That said, cyber security standards pose the risk of over-reliance. According to Thomas Norman, they are "both a solution and vulnerability. While they provide a roadmap to securing systems from multiple points of entry, we should remember that they only protect from known threats."

In spite of the over $88 billion spent on cyber security in 2013—more than double than in 2006, according to the Ponemon Institute–there's no sign that cyber attacks are on the wane. And with little international cooperation and real enforcement, it is incumbent upon the individual CSO and security consultant to keep up with the latest threats and solutions, and better educate customers. Information about new threats can be found in publications such as CSO Magazine and Janes, government agencies' publications, and by simple web searches.

As the world becomes more and more reliant on interconnected computer networks, I predict that the threat of cyber attacks will, unfortunately, increase in volume and severity. I urge you to do whatever needed to not be the next victim.

About the author: *Ayel Vogel is president of AMID Strategies. He has more than 20 years of sales, marketing and management experience in the homeland security* industry. For more information, visit www.amidstrategies..com.

Bigger isn't always better

(continued from page 17)

Small/medium businesses operate on the front lines

Top level executives at big companies are typically not directly involved with customers and everyday management issues. But they are the people making decisions that affect their customers' present and future systems. At small/medium businesses, upper level management is usually in touch with their customers and aware of trends that impact technology implementations. This results from having first-hand conversations with customers and field personnel, auditing service calls and visiting customers in the field.

Owners have skin in the game

Dealing with the owners of a small/medium size company is far different than dealing with employees at big companies. There is no question that the mindset is different from owner to employee. Deal with an owner and you are far more likely to achieve satisfaction as they want you as a customer for life – not for a single sale or project. And ownership mindset often carries over in small/medium businesses to employees who flourish in environments that promote entrepreneurial thinking. This type of corporate culture drives customer service, support and satisfaction best. It's another characteristic that big business strives to emulate that is integral in most small/medium businesses.

There's no doubt that big business plays a critical role in evolving technologies like access control. But small to mid-sized companies strive to retain the small/medium company attributes that have helped its national growth and will serve its continued global growth. By structuring an international network of systems integrators and installing dealers, Galaxy has successfully modeled its customer support and technology development strategies after those which have been applied since its earliest beginnings. The key is to remember that success and growth don't necessarily mean you have to be big or even act big. Treat every customer like they're your biggest customer and the rest will take care of itself.

About the author: *Robert Loughlin is president and founder of Galaxy Control Systems. He is veteran of more than three decades in the security industry.*

Leading the Way in Megapixel Video.

Cutting-edge Innovations
Superior Performance
Broadest Selection of Megapixel Cameras

Protect Your Business While Increasing ROI

Arecont Vision megapixel technology delivers superior image quality and reduces overall system costs by covering larger areas with fewer cameras. Excellent Image Quality + Camera Reduction = Terrific Return on Investment. Megapixel technology provides a new way of monitoring security systems, allowing less personnel to view more at once and zoom in for details of live or recorded video.

- Forensic Zooming
- $ Reduced Overall System Cost
- H.264 MJPEG Dual Encoder H.264/MJPEG
- True Day/Night with IR Cut Filter
- x8 Multi-Streaming
- Integrated Motorized Lens with Remote Focus and Zoom
- WDR Wide Dynamic Range up to 100dB at Full Resolution
- Flexible Cropping

SCHEDULE A DEMO AT YOUR LOCATION!

+1.818.937.0700 | 877.CAMERA.8
avsales@arecontvision.com

Made in the USA

Arecont Vision®

www.arecontvision.com

Leading the Way in Megapixel Video™

Request information: www.securityinfowatch.com/10215742