International Council of Industrial Security & Safety Management

ICISS

Monthly Newsletter

October 2017

# New Trends in Security Management

**The security industry will continue its trend of offering more specific solutions to particular problems, rather than one-size fits all hardware / software.**

## Inside this issue:



The world changes ever faster due to new technologies. But why does it move so quickly? Because industries are changing their needs, the consumers are changing too and the world needs to move in the same direction.

Physical security services are predicted to trend towards offering more specific solutions as well as a higher level of integration and service. The thought is, instead of viewing physical security as a series of connected hardware and software systems, industry experts see a movement towards systems that provide more of a security as a service.

Next year is expected to be the year that will increase the demand for security as a service as a key component of successfully run security operations. In an industry where control is essential and multiple details are going on at the same time, there are Security operations management systems will lead the way.

The control of access to a property or parts of premises is an integral part of any security risk evaluation. Apart from the exclusion of unwanted visitors and intruders, an access control scheme will help to reduce the risk of Industrial Espionage and the potential for Computer Related Crime.

In many businesses there are areas that only selected personnel may access also there may be areas that should only be accessed at specific times. These combinations can readily be catered for by a suitable access control system.

The most essential part of the Access Control System is 'identity'. The positive and most authentic identity of any man or material is essential for access control system.

'False acceptance' is detrimental to security and 'false rejection' is harmful to business and profitability. Therefor concept of integrated "Identity and access management (IAM)" came in to being.

Converged security management is the key to mitigating of new-age security risks.

# New Trends in Security Management … 1

**Exploiting internet of things (IoT) technology without creating cyber-security vulnerabilities is one of the defining challenges in today's security landscape.**

**Just two decades ago, the world's first network camera was launched developing pioneering technology that would later become the enabling concept behind the internet of security things (IoST).**

**Innovations such as these drastically influence the way society and businesses operate and keeping up with these advancements presents many challenges. One of these is ensuring that the new technology implemented by organisations across the world will have the scalability to grow and meet the demands of customers for years to come.**

Presently Identity and Access Management (IAM) is a mature and well understood domain of security. That doesn't mean it's static. While IAM is commonly associated with security - indeed, it is an essential part of a holistic security program - many people are beginning to understand the business processes it represents as well. They therefore view it as an IT operations topic. The truth is likely both: It blurs the lines between security and operations.

Johan Paulsson, Chief Technology Officer at Axis Communications details the reasons why he feels the industry is moving in this direction of security as a service:

1. **Reduce the costs.** "Systems will "not only take away the burden of managing the complex systems involved, but also reduce the costs of keeping those systems up to date and secure". The result "will not only free up internal resources which could be better focused elsewhere, but also improve the service level of the security system and enable better device management".

2. **Specific solutions to individual problems.**
Security industry will continue trending towards more specific solutions to individual problems. Customers look for integrate solutions in one unified system. They want that system to be adapted to their needs and customized based on the site and post. "The end to end solutions could tackle a specific issue". Customized Security as a service (SaaS) systems, provides a key advantage to physical security providers, allowing the supervisors to adapt the system to all possible scenarios and update the reports in real time.

3. **Increase in the use of artificial intelligence.** The security industry will see an increase in the use of artificial intelligence. "The benefits are that although all customers are different, the environments and locations they are based in tend to fall into the same general categories, with people exhibiting the same general behaviours. Once those behaviours have been 'learned' the patterns that underlie them can be shared, enabling the system to flag up when

# New Trends in Security Management … 2

**Security personnel are doing more complex duties now…**

**More are more soft skill are needed of them…**

**Just Technology is not the only solution. Right mix of Security aptitude and attitude is must.**

**Innovations are taking place at break-neck speed and technologies' shelf life has decreased.**

According to another interesting article "6 trends to watch in the security guard industry" from propertycasualty360, we can find other relevant trends for the security industry in next year.

**4. Expanded responsibilities.** "Security guard firms are contracted to protect people and property in a wide variety of industries". The firms are starting to be asked to provide additional services outside of security, and this trend will increase in 2017. A multifunction and customizable software can completely avoid communication or dispatch issues for these companies, as they will be able to adapt the software to each customers' growing needs. The companies will be able to keep all incident and activity reports centralized and categorized in a digital logbook.

**5. Remote video monitoring.** Customers contracting security firms are increasingly asking for remote video monitoring. They believe that even though there is a high initial investment on equipment, it will reduce costs in a future.

**6. Increased specialization.** Security firms used to work with a big variety of clients. Nowadays, the trend is to specialize in industries such as schools or hotels. This can also differentiate you from your competitors.

**7. Beyond video.** We know that physical security doesn't just involve surveillance of people/places/objects. It is also about physical access control, one and two-way communication and managing emergency situations – and often managing this from a significant distance.

So, to extend the concept of integration even further, 2017 should be the year when security cameras work hand in glove with intelligent doors, intercoms and speakers, both locally and remotely. That means one simple system that can manage them all, in real time – enabling customers to see, hear and talk to the people in/near their buildings.

The trends indicate that the industry is following this path of offering security in addition to other services. Specialization and customization are the stars the next year. Therefore we will see an increasing demand from security providers for customizable Security Management Software that will provide an easier way to manage the security operations.

If a security team can achieve these things, they are well-positioned to leverage offshore or outsourced resources to manage these configurations. This allows the core security team to refocus on more pressing and complex issues.

While many changes in the security domain make our lives more difficult, the changing IAM landscape continues to improve business outcomes, improve the user experience and increase operational efficiency.

# Opportunities for Security Industry

In monitoring, surveillance and alarm management field, the data storage and retrieval is big challenge. The cost effective Security management in this area can be achieved through four essential activities. Technologically, all the tools are available. Now it's time to use them. Adopting a cloud-based IAM solution is not something to be taken lightly, especially if there are significant investments in on-premises licenses, infrastructure and operations. If these investments exist, the next upgrade or expansion cycle is the time to look at moving to cloud-based IAM (Identification & Access management). Doing so makes it possible to adopt standardized solutions, simplify operations and reduces operational cost, all while using the leading-edge technology.

1. Identify your most valued assets (e.g., data, applications, etc.).
2. Identify and integrate privileged user repositories to understand who these users are.
3. Collect activities on critical infrastructure in the central Security Intelligence and Event Management (SIEM) solution.
4. Identify expected activities for each user type and create runbook use cases to respond to events that are outside of these.


Adopting a cloud-based IAM solution is not something to be taken lightly, especially if there are significant investments in on-premises licenses, infrastructure and operations.

If these investments exist, the next upgrade or expansion cycle is the time to look at moving to cloud-based IAM.

Doing so makes it possible to adopt standardized solutions, simplify operations and reduce operational cost, all while using the leading-edge technology.

**Capt. SB Tyagi, COASÇC, FISM, CSP**

The global IP camera market is expected to reach $9.2bn by 2020, proving firms are beginning to expand the ways they use internet -connected technology.

We expect to see next year as the year when these new camera capabilities are combined with real-time

analytics to address several security challenges, including facial recognition, forensic analysis and perimeter protection.

# 2017 Threats Predictions: IT / Cyber Security

The 2017 threats predictions run the gamut, including threats around ransomware, sophisticated hardware and firmware attacks, attacks on “smart home” IoT devices, the use of machine learning to enhance social engineering attacks, and an increase in cooperation between industry and law enforcement:

1. Ransomware attacks will decrease in volume and effectiveness in the second half of 2017.

2. Windows vulnerability exploits will continue to decline, while those targeting infrastructure software and virtualization software will increase.

3. Hardware and firmware will be increasingly targeted by sophisticated attackers.

4. Hackers using software running on laptops will attempt “dronejackings” for a variety of criminal or hacktivist purposes.

5. Mobile attacks will combine mobile device locks with credential theft, allowing cyber thieves to access such things as banks accounts and credit cards.

6. IoT malware will open backdoors into the connected home that could go undetected for years.

7. Machine learning will accelerate the proliferation of and increase the sophistication of social engineering attacks.

8. Fake ads and purchased “likes” will continue to proliferate and erode trust.

9. Ad wars will escalate and new techniques used by advertisers to deliver ads will be copied by attackers to boost malware delivery capabilities.

10. Hacktivists will play an important role in exposing privacy issues.

11. Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime.

12. Threat intelligence sharing will make great developmental strides in 2017.

13. Cyber espionage will become as common in the private sector and criminal underworld as it is among nation-states.

14. Physical and cybersecurity industry players will collaborate to harden products against digital threats.

“To change the rules of the game between attackers and defenders, we need to neutralize our adversaries’ greatest advantages,” said Vincent Weafer, VP of Intel Security’s McAfee Labs. “To overcome the designs of our adversaries, we need to go beyond understanding the threat landscape to changing the defender-attacker dynamics in six key areas: information asymmetry, making attacks more expensive, improving visibility, better identifying exploitation of legitimacy, improving protection for decentralized data, and detecting and protecting in agentless environments.”

# How a Security/Guarding Company Can Stay Competitive and Win New Business ...1

There are a lot of security providers on the market today, and with all of those options, it can be tough for a company to set itself apart from the countless others and win new clients. What follows are some strategies and tools that can help you not only win new security/ guarding business but also help you keep the clients you have.

**Positioning**

One of the most important things you can do in your strategy to win new business is to determine your specific market. It's probably not likely that your company can serve every industry and business type. Find out which businesses it makes sense to work with and go after those markets. In general, you cannot be all things to all people. Experience has shown that companies that specialize in meeting the needs of one group of consumers over another tend to be more profitable.

**Being Found**

Another item you can add to your strategy to win new business is to simply maximize your chances of being found by new clients. Your goal is for your potential clients to perform a Google search for your particular service and find your company towards the top of the list.

There are a few things you can do to improve your odds of that happening. First, make sure your business has its location listed on Google, as well as other business listings. This way, Google will show your contact information when someone queries your business. It also means it's more likely your business will be listed when someone in your area searches for the services you offer.

You should also focus on including quality, local content on your own website. Make sure the content is unique and relevant to your target customers–remember, you're trying to set yourself apart from the competition. Fresh content added at least once per month will also help your company rank better in search results.

It's vital that your company take an active role on social media platforms as well. Complete profile pages for all the major social networking sites where your target customer is likely to be engaged, making sure your pages public. This will help boost your findability in search engines as well as help sell your services. Make sure, however, that you post fresh content on those sites on a frequent basis.

One final tip to ensure your business is easily findable in a search engine is to make sure your website is mobile friendly. Work with your webmaster or IT department to make sure your website comes across clean-looking and error free when viewed from a mobile device.

**Be the Solution**

Prior to going into a pitch, it's important to understand how consumers work and what they're looking for. Your potential clients aren't looking for products–not really. What they're looking for are solutions. Solutions solve problems, so ultimately you need to understand what those problems are.

# How a Security/Guarding Company Can Stay Competitive and Win New Business … 2

**The most important thing you can do in your quest to earn new business:**

**Ask questions.**
Walking into a meeting with a client and launching straight into all of the features your company has and how great they are, blah blah-blah, is actually a solid way to lose that potential client.

The smarter approach is to ask questions right off the bat. Ask the client what they're looking for in a security provider and what their biggest security concerns are. If you open the floor like that and allow a client to do most of the talking, you'll be told everything you need to know.

The key is to use all of the information you learned regarding your client's problems and show them specifically how your company can be a solution.

**Stand out from the crowd.**
To become a successful business in a sea of competitors you have to show that you're a unique value to new clients. There are a LOT of competitors in the security provider field, so it's extremely important to show a potential new client what your company can provide that a competitor cannot.

Part of that pitch will take some serious introspection on the part of the security company. A bigger (and easier) part of that pitch can come from the specific tools your company provides. While those tools might not be 100% unique, how you use them and the value you provide can be.

Ultimately, you'll need to show the company you want to work with what's in it for them.
http://www.trackforce.com/securityguarding-company-can-stay-competitive-win-new-business/

# Security Executives Need to be Good Salesmen! .1.

One of the most important yet often overlooked factors in high-end, private sector protective operations is the sale. It is very difficult getting the right decision-makers to sign onto security budget – and to be willing to pay for it. One of the biggest challenges is that in most cases, the decision-makers who are in position to sign onto security program aren't security professionals. So the challenge is how to communicate – and sell – security to non-security personnel.

Having acquired over three decades of experience in this field I know there are many opportunities which Security Chief can obtain to make his case for expenditures on new security initiatives. These cover executive presentations, security board meetings, budget committee meetings and even one-on-one conversations with executives of key functions.

**Make it Simple!**
There's a celebrated quote attributed to Albert Einstein that goes "If you can't explain something simply, you don't understand it well enough". Most executives and stakeholders are probably familiar with this idea, and you would be wise to familiarize yourself with it too. It's OK, or even necessary, to elaborate on a subject, especially if you're asked to do so. But don't forget to start with a simple explanation before you plunge into the deep-end of things.

It's very common among security professionals to make fun of naive clients and executives who are so ignorant about their own safety and security. But try not to let this mostly harmless tendency infect the way you explain security to them. Remember, the executives and decision makers you are talking to did not get where they are by being dumb, and they're not going to appreciate you treating them as such. Security just isn't their field of expertise, it's yours.

The idea is to synthesize and summarize things into understandable terms with actionable outcomes. It's the opposite of dumbing things down.

**Know your audience**
This one comes up a lot. You've put together a great security presentation; detailing threat matrixes, risk mitigation strategies, hostile planning disruptions, attack contingencies, and, oops… You've lost your non-security audience about thirty seconds into it.

Always be mindful of your audience's level of understanding and/or caring in regards to security issues, and adapt the way you explain things to suit them. It's like the old basketball idea, where the responsibility for the pass falls on the player who throws the ball, not on the one who fails to catch it. Your listeners are where they are. It's your responsibility to pass the information to them at a level they can receive it.

# Security Executives Need to be Good Salesmen! .2.

Finally, on the slightly negative end of things (which means you should never start off with this angle), if your audience is reluctant to take action, try to explain that a lack of preventive and/or reactive security capabilities opens them up to certain legal liabilities. It's not the most cheerful subject to raise, but one that might sway the legal department to take a second look at your suggestions.

**Return on investment (ROI)**
You might be able to wow every decision-maker on the planet with your tactical skills and experience, but if they don't see what's in it for them, they're not likely to invest any capital in it.

As you explain things, always keep your audience's interests in mind – not where you think their interests ought to be, but where they actually are right now. The bottom line for almost any decision-maker is **'How much will it cost me, and what's in it for me?'** It's in the second part of this question – the return on their investment – where you should really put some explanatory effort.

- Cost of Security v/s cost of having 'no security
- Cost of having 'No Security' v/s cost of having reasonable security
- Cost of having effective security

**Shock & Awe: A failed tactics in Corporate World**
Though this can, on occasion, lead to a sale, shock & Awe tactics aren't usually effective. It's a classic mistake that many security professionals make – trying to scare decision-makers with horrific case studies, and doom-and-gloom prophecies of what might to happen to them if they don't employ some immediate protective measure.

It's not a question of describing what you think is objectively true, but choosing an effective way to communicate things in order for your listeners to take action. As strange as it may seem, most people are not likely to take action if you try to shock and scare them. Doom-and-gloom just doesn't sell very well. You don't have to mindlessly sugar-coat everything; just find a more effective way of getting your audience to want to take action.

**Put things in relatable terms**
Once you know who your audience is, try to translate security into relatable terms your audience is not only familiar caring about, but familiar paying for.

It's not that it's particularly difficult for decision-makers to understand ideas like security risk mitigation, it's just that it's a stretch for many of them to give it the budget it requires.

But put it in relatable terms for them, and explain that a risk mitigation strategy is actually a potent insurance policy (with preventive and reactive benefits), and presto, every single person in the room, from accountants to HR managers can relate to it.

Speaking of insurance, suggest to your budget conscious audience (I've yet to meet one that isn't) that they can inform their insurance provider about their new security measures, and see if they can negotiate lower insurance premiums to cover the now lower risk profile – thereby actually saving them money.

# Security Executives Need to be Good Salesmen! .3.

**Manage expectations**

A few years ago I was asked to speak to the staff of a wealthy San Francisco Bay Area foundation. Before I was contacted, the foundation (which had received a number of threats) had initially asked their local police department for some security guidance. Their local PD then sent an officer who promptly started teaching the office staff (mostly consisting of women) hostile defensive tactics such as turning your side to an armed attacker (in order to decrease the size of your silhouette), before employing some nifty handgun disarming techniques to neutralize the threat.

Needless to say, this did not go over too well, and the now terrified staff wanted to get a slightly more realistic second opinion.

I'm sure the officer had the best intentions, but he just didn't set realistic expectations for his non-law enforcement, non-security audience. It's not a question of objective tactical effectiveness, but of relatable and realistic ideas to suit your specific audience. To ignore this point will not only be a disservice to your audience, but might get you booed or laughed out of the room. "I don't know"

Last but not least, if a question gets asked that you don't feel qualified to answer, don't be afraid to say "I don't know".

I know many security professionals who are afraid this will make them look weak or ignorant in front of clients or prospective clients (and I can admit I also had this issue till I got over it). The fact of the matter is, however, that no one knows everything, and it's actually important to admit what you don't know.

Philosophers and stoics since ancient Greek times have referred to Socratic Ignorance (the frank acknowledgement of what you don't know) as a true sign of wisdom. Not only is there no shame in admitting you don't know something, it can be a way to demonstrate integrity and intelligence. Don't make a big deal out of it, just admit you don't know, and offer to get back to the person with an answer later on.

There are obviously more than just these tips to be given on this topic.

# What ICISSM is All About?

ICISS is purely non-commercial forum for security and safety professionals world-wide! It neither is with any support from any business groups nor is it projected by any business house in the back-ground. All its members have no stake in any solution providing or consultancy firms. Their association with ICISS is totally based on mutual benefit of knowledge sharing and networking.

We welcome all the security and safety professional world over from diverse background and encourage them to interact freely by asking the questions, replying them or by sharing their knowledge and experience. The council also strives to have strategic alliances with similar forums world over for furtherance of its objectives. Formed in 2010, the Council is totally a-partisan, apolitical and does not represent any pressure group or interest group.

ICISS strives not to provide surrogate platform for anyone to enhance their respective business interest. It is thus totally professionals' body aimed at, 'professionalizing the professionals'!

We in ICISS believe that having different view than the majority is not bad! In fact we encourage difference of opinion and take every different views as intellectual stimulus to either convince or get convinced – either way both the parties are benefitted! Those who dare to think differently have shown that firstly they can think and secondly they are not overawed by the majority views! Such are the traits of 'Thought Leaders' and they deserve our respect!

For more details on our activities, please visit us at - http://onlineicissm.wix.com/iciss

# What ICISSM can do for you?

ICISS

**111 – GAIL Society, Sector Pi (I&II),**
**Near Eldeco Riviera, Greater Noida,**
Gautam Buddh Nagar, UP
**Mails:** onlineicissm@gmail.com
**Blog:**
http://captsbtyagi.blogspot.com
**Web-site:**
http://onlineicissm.wixsite.com/iciss

**Consultancy:** International Council of Security and Safety Management (ICISS) would be happy in providing consultancy to Corporates on all matters relating to Industrial Security Management from the best security professionals as it has on its panel the very best security professionals from almost all over the world. We have accredited security consultants from India, South Africa, UK, USA, UAE, Belgium, Libya, Yamane and Austria to name few countries. All the security consultants are under oath not to represent any solution provider or system integrator, thus their consultancy and recommendations are most impartial.

**On-site Security Survey and Audits:** Conducting on-site security surveys and audits is the forte of ICISS. Its specialists have carried out numerous such surveys which were beneficial to clients in improving the security preparedness and also in cost-cutting. .

**Contents Delivery: The** experts of ICISS help the Clint in developing its plans, prepare manual and prepare various forms and formats to be used for every day security &safety functions. It will also help the Clients to develop the training contents such as write-ups and the presentations. The specific needs of specific niche segment of the industry will also be met by ICISS.