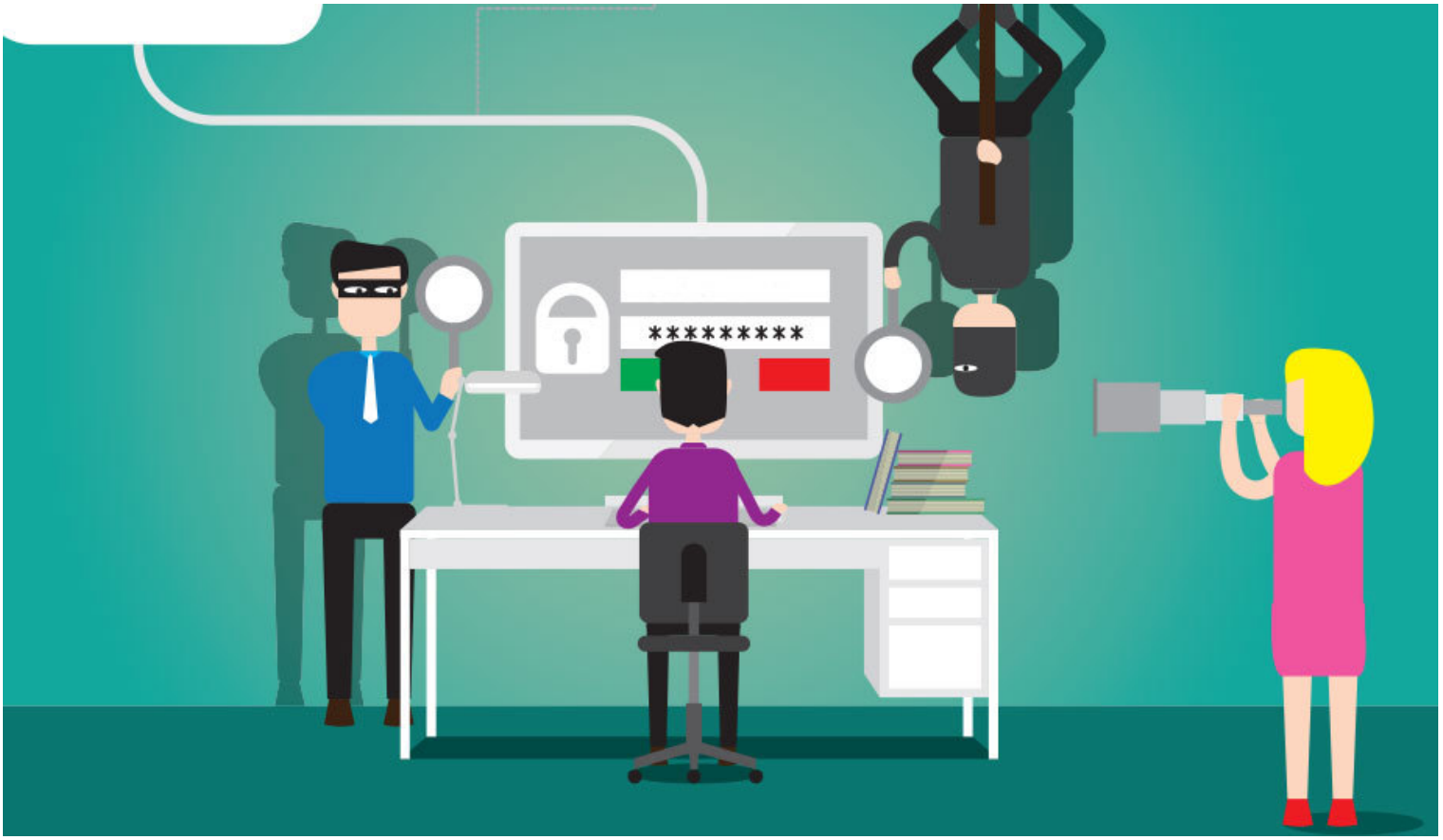
securityinformed.com
Making The World A Safer Place

Security Industry Trends To Be Led By Focus On Cyber Security In 2019

Published on 24 Dec 2018



The Security Industry Association (SIA) looks forward to 2019, and it is apparent that physical security is moving into its most formative years. Changes presented by emerging technology, open systems and growing connectivity among devices and sensors will make a big difference for manufacturers, systems integrators/dealers and end users.

With a more open, connected environment come cyber risk and data privacy concerns – which is why, in SIA's 2019 Security Megatrends, cybersecurity's impact on the physical security industry ranks number one on the list. Cybersecurity is affecting all areas of the industry landscape, from security implementation to attracting top talent to the workforce.

Digital Transformation

The digital transformation we are experiencing impacts many other parts of the security industry as well, bringing opportunities like evolving identity management and collecting and delivering big data to customers. At this critical point in the industry's development, it is important to embrace change, leverage disruptive technology in ways that give companies a competitive advantage.

> To determine this year's Megatrends, SIA surveyed hundreds of executives from member companies

To determine this year's Megatrends, SIA surveyed hundreds of executives from member companies, along with current and recent Securing New Ground speakers and attendees, to identify which previous trends were still relevant, which trends were no longer as impactful and which broad trends should be added to our report.

This Year's Security Megatrends

1. **Cybersecurity's Impact on Physical Security**: It is important to prioritise cybersecurity for your business, your customers' business and the vendors with which you work. This trend calls for continual process improvement and investment.

2. **Internet of Things (IoT) and the Big Data Effect**: The security industry makes use of IoT, analytics, artificial intelligence (AI), robotics and more, and data is coming from everywhere. The industry now faces the challenge of effectively managing and segmenting this information to be pertinent to the user.

3. **Cloud Computing**: Cloud platforms and applications are becoming prevalent across security solutions. This technology helps security integrators provide managed services and the advantages of off-site systems and services to customers.

4. **Workforce Development**: With historically low unemployment, finding skilled employees is a challenge to the whole security industry. Security stakeholders need talent with IT, cybersecurity, AI and even privacy expertise, presenting a need to grow students' interest in the industry.

5. **AI**: Research firm Gartner predicts a new "democratisation of AI" that will impact more organisations than ever before. Companies are now testing this technology before offering it to customers and exploring how AI data can be used to improve security threat assessment and response.

6. **Emphasis on Data Privacy**: Growing connectivity brings new concerns over data privacy. Finding the balance between security and convenience is a dilemma the industry must now address.

7. **Move to Service Models**: The newest home security technologies are strongly impacting installing companies. Systems integrators must find ways to focus on services customers want and need and move to managed service models to make up revenues.

8. **Security Integrated in Smart Environments**: As everything becomes connected, smart environments will begin to proliferate. Buildings and cities are becoming more conscious, with connected systems now able to automatically respond to and even anticipate the needs of facility users and citizens. We must continue to find ways to make these environments smarter and safer.

9. **Identity of the Future**: With facial and voice recognition and biometrics growing in popularity and appeal, how will we enter buildings and access networks tomorrow? The industry will anticipate and adapt to constant technological change in identity and visitor management.

10. **Impact of Consumer Electronics Companies**: The influx of consumer electronics companies and DIY systems means changing rules and players in the security industry. This disruption presents both challenges and opportunities for security companies.

Author Profile

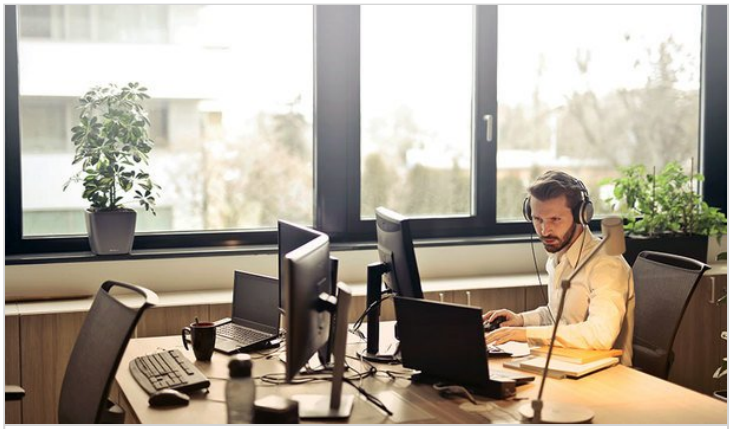
Scott Schafer

Scott Schafer is chairman of the board of directors for the Security Industry Association (SIA) and the principal/CEO of SMS Advisors, a security consulting organization with a focus on improving growth and profitability. An experienced senior executive, he has previously worked with medium-sized and large technology companies including Arecont Vision, Pelco/Schneider Electric, Reynolds & Reynolds and NCR/AT&T, and he currently serves on the board of advisors of several high-tech security companies.

You may also be interested in...

Five Best Practices For Protecting Video Surveillance Systems Against...

There’s no denying that cyber-crime is one of the biggest threats facing any organization with the devastating results they can cause...



Five Cyber Security Threats Your Enterprise Must Address

By now your organization should know the drill. To keep your enterprise safe from unauthorized access you take the basic precautions: create...

Preparing For Cyber-attacks: The Intersection Of Cybersecurity And Phy...

Terry Gold of D6 Research has been giving “cyber in physical security” presentations at a variety of conferences, including ISC...

Watching Trends In Real-Time: SecurityInformed.com's Top 10 Click-Wort...

Timely and important issues in the security marketplace dominated our list of most-clicked-upon articles in 2018. Looking back at the top ar...

Beyond Cyber Security: Why Physical Security Must Be A Key Element Of...

Edward Snowden’s name entered the cultural lexicon in 2013, after he leaked thousands of classified National Security Agency documents...