Reading Tomorrow's Security Landscape



As a security professional, you're always on the lookout for insight on emerging security trends and for strategies to identify and control risk.

A recent Freedonia Group industry report ("Industry Study 2675, Private Security Services") identifies some of the trends that will have the greatest impact on the security industry through 2014.

Here, Pinkerton experts discuss that changing landscape. They also address the latest thinking, the new risks, and the technology you can tap as you shape your security strategy.

Trend #1: Employee Screening

A decrease in the unemployment rate and employers seeking deeper employee background checks, along with greater liability concerns and more complex regulations all are combining to fuel demand for preemployment screening.

In fact, the Freedonia Group anticipates that through 2014, pre-employment screening will be the fastest growing security service segment.

What's Driving the Trend

There's a greater emphasis on safe workplaces and an emphasis on the quality of the employee itself, according to an executive of Employment Screening at Pinkerton. As a result, he finds that companies not only are performing pre-employment screening, but some even are re-screening existing employees on some kind of regular schedule.

Deeper screening: "Clients are recognizing there are different types of searches available that can reveal much more information and that inexpensive searches don't necessarily give them the level of investigation they may want," they coment. In addition, employers are bowing to pressures from insurers and state regulations that often demand more comprehensive employee background checks.

Deciphering data: "Employers need to understand what their obligations are in terms of usage of the information that's returned to them," they comment. Data from local, state and federal jurisdictions are returned in multiple formats, so it's often difficult to understand what the records actually are, what they mean, and how and if a company can use the information.

Subject matter expertise: Companies need to stay abreast of hiring trends and myriad rules and regulations. Yet many don't have in-house subject matter experts to keep up with those changes or to ensure that they're performing the necessary searches.

For example, in light of new EEOC guidelines, it is now more important to analyze the nature and gravity and job relatedness of an offense in determining the overall eligibility of a prospective employee. In comparing state law meanings, for some states driving with an expired driver's license is a misdemeanor and in other states, it's a felony.

"Employers are always looking for someone who can provide support for the legal and compliance requirements that they have," they explain.



Chris Hammond, Global Director, Physical Security Technology for Pinkerton, has over 25 years of experience with physical security systems.

Keeping up with change the executive points to the dynamic, fluid nature of rules and regulations, as well as the complexity associated with ensuring that companies' procedures and policies are best practiced and meet compliance requirements. "We help clients navigate those complexities and meet the proper due diligence in a cost-effective manner," they say.

Trend #2 Security Consulting

White collar crime, such as embezzlement, industrial espionage, and computer crimes, is just one reason the market for security consulting services is expected to increase by 6.9 percent annually through 2014.

Pinkerton, too, finds that security consulting is on clients' radar and it's seeing greater demand for such services. Services can range from delivering advice on access control to assessing hiring policies and developing crisis response procedures.

Drivers of security consulting growth

Because of budget cuts, many companies don't have the funds for in-house security experts, according to an executive of Central, USA for Pinkerton. Such firms are looking to outsource everything from computer security to workplace assessments. Similarly, mid-sized businesses and institutions without in-house security departments also look for outside help.

Companies expanding overseas often tap a security consultant with a global scope to analyze on-the-ground risks and develop a security management strategy appropriate to a given industry and to the challenges presented in a particular country.

Identify weaknesses

Businesses experiencing losses, whether in a retail environment or on a manufacturing floor, want to determine why profits are walking out the door, and this often leads to contracting with a security consultant.

The consultants typically begin by analyzing and understanding a company's procedures; sometimes they might even put an undercover investigator in place.

Frequently, finds the executive, there's no theft or dishonesty at all. Losses often stem from operational shortcomings that can be solved with tweaks to internal procedures and policies. Profits and losses.

Security consultants can improve a company's bottom line by identifying and preventing activities that negatively affect profit. "If you have an employee selling trade secrets or company information, whether that be client lists, research documents, or prototypes for new services and products, that can impact your current earnings and future revenue," observes the executive.

Trend #3: Systems Integration and Management

"Everyone is looking at reducing business costs," says Chris Hammond, Global Director of Physical Security Technology for Pinkerton. For many, that entails tapping electronic security systems integration and management services. The market for such services (excluding home automation) is projected to advance 8.6% per year through 2014.

Security is more integral to businesses — now an expectation — than it was 10 years ago, and it's getting far more complicated, according to Hammond. As a result, companies are looking for more complete, managed solutions.

"Companies need to stay abreast of hiring trends and myriad rules and regulations."

Greater intelligence

Camera systems, for example, were once used as evidentiary tools, giving investigators clues about an incident after it occurred.

Because of technological advances in remote video monitoring and video analytics, for example, companies are seeing greater value in making such security investments. Why? They can prevent something from happening or know about an incident in real time.

"Between physical access control and video systems becoming more intelligent, there's more you can do with security technology than in the past," says Hammond. "The technology now can show some return on the security investment."

Unexpected benefits

"Consider how a security system can affect pieces of your business that aren't directly related to obvious things, like burglary," suggests Hammond.

Video surveillance, for instance, can reduce business losses because staffers know they're being monitored live. It makes people who are honest feel safe and dishonest people uncomfortable because they have no idea when they're being watched and who's monitoring them.

Moreover, the enhanced security has the potential to lower employee turnover and its associated costs. Problem employees don't want to work in secure, monitored workplaces because they see no opportunity

to supplement their income. And a company can eliminate the waste associated with hiring and training and then firing dishonest employees.

Industry evolution

"Companies need to realize that industry advances have created a whole world of new possibilities," says Hammond. "Today's security solutions can have an impact on businesses in ways that are completely different than they were just three years ago, and companies can see measurable returns on their security investment."

