

Powerful Combination

The corporate security service is gaining momentum in our country as a standalone practice. It has obvious differences from the conventional offering as it is situated at the intersection of different disciplines, including financial, IT and cyber-security, corporate governance, compliance, criminal defense, GR. The risky areas formulate requirements for a comprehensive solution of an array of security factors. **Sergey Pogrebnov** and **Sergiy Smirnov**, partners at **Sayenko Kharenko**, gave us their vision of a powerful combination to ensure business security.

UJBL Would you agree that corporate security is mostly a Ukrainian and post-soviet trend rather than something taking place in developed countries?

Sergey Pogrebnov: No, I don't. If we compare the history of business security in the West and in our country, we'll see obvious differences. Firstly, this is in the terms of the existence of middle-class or capitalist societies and economies, as well as the rights to private property and entrepreneurial activity.

If we consider the date of the complete victory of the Dutch Revolt in 1648 to be the date of the emergence of business protection as a phenomenon and profession, in the West, this history is at least 300–350 years old. This is only in the bourgeois capitalist period, which is more or less similar to modern economic and legal relations. The profession has been developing all this time, accumulating its knowledge and traditions.

In our country, the bourgeois and capitalist society was destroyed in 1917 and business protection-related traditions were interrupted before 1986 when the cooperative movement began to develop. Entrepreneurship has been officially revived in Ukraine since 1991. The traditions, experience, theory, methodology, and techniques for the protection of Ukrainian business have existed in modern Ukraine for no more than thirty years at best. Before that, only one type of security existed in Ukraine — state security in its worst form, that of a totalitarian state.

The different development histories of the economy, entrepreneurship, and security led to the formation of completely different approaches to business security in the West and in the former USSR. The development of private (economic) security is inextricably linked with the development of the economy.

Ensuring enterprise security in foreign economic theory and practice is associated with two distinct aspects: *Enterprise Security* and *Risk Management*. The term *Enterprise Security* implies the physical protection of an enterprise (engineering and power tools), methods of competitive intelligence, information protection, and the concept of *Risk Management* including the economic aspect of managing security factors.

The development of corporate management required the development of new approaches to risks based on the one hand on strengthening the control of companies by the top management and, on the other hand, on various forms of management integration.

Business protection has transformed from risk prevention into a new tool for competitive advantage.

Sergiy Smirnov: It should be noted that many foreign countries have been thoroughly involved in the study of risk identification, analysis, and assessment for over thirty years.

What has happened in our country in the area of private security in the last thirty years?

Firstly, we had to develop the theory and practice of business security in just thirty years, which is ten times faster than in the West. Secondly, because of our historical heritage, we started from a different position. Until now, most security services employ retired or reserve law-enforcement officers. It must also be taken into account that business security develops along with the business itself. Prior to 2002, security services performed standard protection functions. Starting from 2003–2005, when businesses started to face raids, the principles and best practices of corporate governance emerged and began to develop. Since 2005, studies on the development of corporate security theory have also emerged in Ukraine.

S. P.: The activation of foreign capital in 2005–2008 and the creation of numerous companies with foreign participants also influenced the development of the business protection sphere.

Today, corporate security in Ukraine is developing exponentially. The old school of private security accepts, introduces, and develops new principles of effective corporate governance, when the security service becomes a business unit and compliance, forensic accounting, PR, and GR take their place in the business protection system. In security structures, KPI is undergoing introduction with security issues raised to the level of company Supervisory Boards.

Nevertheless, in Ukrainian business, there are no more than 1-2% of enterprises

SAYENKO KHARENKO



KEY FACTS

SAYENKO KHARENKO

Year of establishment: 2004

Number of lawyers/partners:
100/14

CORE PRACTICE AREAS

Antitrust & Competition
Banking & Finance
Bankruptcy & Debt Restructuring
Capital Markets
Corporate & M&A
Corporate Security
Government Relations
Intellectual Property
International Arbitration
International Trade
Labour & Compliance
Litigation
Private Wealth Management
Real Estate & Construction
Tax
White Collar Criminal Defence



Nevertheless, in Ukrainian business, there are no more than 1-2% of enterprises which have deployed corporate security structures for the whole market

with deployed corporate security structures.

In most enterprises, security services continue to operate that have all the flaws of old policies and standards without taking into account modern corporate security requirements.

UJBL Corporate security is a multifaceted offering that includes not only pure legal services. What is the core reason when a corporate security system is introduced to a business?

S. S.: The world is changing irreversibly at an alarming rate. The demands facing any business and its owners to protect themselves, and their desire to ensure stability and a sustainable future, are also growing.

Technologies, the Internet, and gadgets are developing; pseudo-artificial intelligence and robotics are becoming increasingly popular in our lives; new industries and virtual currencies are appearing. Criminality is changing as well: new types of crimes are emerging, including those that seemed fantastic yesterday.

An ongoing undeclared war, two revolutions in ten years, radical changes to legislation, the reform of the state, judicial, and law-enforcement bodies, and the emergence of new law-enforcement bodies, as well as the signing of the groundbreaking EU-Ukraine Association Agreement and entrance into new international markets, also influence these processes.

The large number of positive and negative influences on the business climate in a very short period of history gives rise to the need for increased requirements for corporate security and the protection of assets. Today, there are about 30 different forms of security and businesses want to have a single entry point to the entire issue.

This entry point is available via a corporate security system developed and implemented individually for each customer.

UJBL What kinds of professionals are involved in providing a corporate security service?

S. P.: When I am asked what corporate security is, I usually answer that it is everything! Corporate security includes not only pure legal services.

I divide the professionals involved in corporate security processes into internal (working for the company itself) and external (providing outsourced services in the field of security).

The internal security system should include all the company's employees: the cleaners, specialists in financial and economic security, security guards, personnel security, information and IT security, competitive intelligence, and trustees to members of the Supervisory Board in charge of corporate security, legal work, and compliance.

Regarding external specialists or external advisers, we recommend recruiting professionals in the following areas: attorneys' office, cyber-protection, corporate intelligence, forensic accounting, crisis communication, information protection, security structures, detective organizations, family security, troubleshooting, and GR.

Only a combination of internal and external professionals is able to ensure the corporate security of the company with the maximum result, especially in a crisis such as raider attacks, criminal proceedings, corporate conflict, the sudden death of the owner and subsequent inheritance, acquisition of uniform-sized business, building of new business processes, and so on.

S. S.: I want to draw particular attention to signing an agreement with an attorneys' office that includes a criminal defense practice. It is ideal when this practice has previous experience in anti-raider protection, corporate law, judicial practice, and, preferably, forensic accounting, as well as experience in dealing with foreign customers. It should be noted that working with white-collar crimes is very different from general criminal practice and working with foreign customers, as a rule, expands the tools protecting the interests of customers outside the *Criminal Procedure Code*. The experience of criminal defense lawyers in the above practices significantly increases the likelihood of a successful outcome of this protection. The absence of such an agreement indicates a significant "breach" in your security system.

UJBL What is the role of the legal adviser?

S. P.: In our case, in 100% of projects with crisis situations we acted as legal advisers

who coordinated and were responsible for the corporate security of customers.

In a number of cases, they submitted their internal services and departments to us in order to build a corporate security system. We then deployed this structure within the company.

In some companies, directors of legal departments head corporate security committees. On the basis of this, you can evaluate the legal adviser role yourself.

UJBL So who actually leads the corporate security service – lawyers or internal security professionals?

S. P.: Both, in fact. In large companies, the specialist who is responsible for corporate security is a member of the Supervisory Board, oversees legal practice, business security, compliance, and risks. In smaller sized companies, a member of the Management Board or the Board of Directors should be responsible for corporate governance. In companies of even smaller size, business security is provided by the security service in conjunction with the legal department. In the third case, we cannot talk about a corporate security system since it lacks a number of management elements. I also know a number of companies where there were conflict situations between lawyers and security personnel, which resulted in virtually a complete lack of business security for these companies.

We have to remember that in crisis situations, lawyers represent the company formally and openly, while security services prefer to act non-publicly.

In the global corporate security system of a holding or a corporation, lawyers and security personnel are only individual participants, though remaining important among all the other units involved in business protection, day-to-day operations, and development.

I also know several companies with a corporate security system built on an agreement with an external adviser, while his/her status in the company is high enough because he/she is also a personal adviser to the owner. In these cases, all departments of the company provide corporate security together with the adviser. Today, this scheme is the most effective and we believe that corporate security should follow this format: external adviser – owner security – business security.

In our case, advisers are lawyers and attorneys experienced in military service, law-enforcement and corporate security services, who use the entire arsenal of



Security had to grow with business, protecting it, studying corporate governance, crisis PR, GR, and some more areas that had not been the focus of the security area before

means of Sayenko Kharenko Attorneys' Office.

UJBL What are the reasons behind such rapid development of corporate security in our country?

S. P.: As I said, there are several of them, and it is rather difficult to single out just one.

The development of the economy, the arrival of foreign investment, banks, and enterprises with their experience, culture and new practices, technologies, methods, and procedures have provided an impetus for the Ukrainian market to develop business security from the physical and technical to the intellectual, technological, and corporate levels.

It should also be taken into account that, along with the growth of the economy, criminality has become more active. At some point, crime transformed from purely criminal into intellectual. The period from 2000 to 2008 is called the years of intellectual corporate raiding. Security had to grow with business, protecting it, studying

corporate governance, crisis PR, GR, and some more areas that had not been the focus of the security area before. Today, it is not enough for a person engaged in corporate security to have a basic education; he/she must be a generalist, have a business education, understand corporate governance, be familiar with the law, master modern technology in the field of security, and become a top manager.

S. S.: In addition, over the past fifteen years, criminality has completely changed its face. Today, white-collar crimes have become the No. 1 problem for businesses.

Fraud, embezzlement, waste, manipulation with powers of attorney, charters, and accounting, and abuse of authority all result in hundreds of millions of dollars in losses. Due to this, forensic practices have grown in demand. A year ago, 85% of business leaders and even many members of the Supervisory Boards of corporations and holdings did not know the meaning of the word.



Business structures that ignore the need to study, implement, and continuously develop the best practices of corporate governance may sooner or later cease their activities or be lost to their owner

S. P.: Until recently, nobody could imagine that cyber-attacks would become so large-scale and ruinous for business. Companies with no cyber-defense were puzzled with the issue after the Petya malware incident.

Another reason that has never been taken into account by the overwhelming majority of the country's security service providers is war. Both security personnel and corporate security systems had to urgently rebuild their work.

This was especially acute for enterprises that had assets in the east of Ukraine, in Crimea, or had stable economic ties in these occupied areas. Our private security services have never had such experience before, maybe except for individual leaders who had combat experience in the past.

S. S.: Changes in legislation can also include the emergence of new structures such as NABU, SAP, SBI, and the Higher Anti-Corruption Court.

The possible legal consequences of these structures' operations for business should be considered when building corporate security systems, increasing the impact of compliance procedures in business structures, and when conducting educational and preventive measures to combat corruption within companies.

S. P.: Changes are taking place in Ukrainian legislation, in European legislation, and beyond. In some cases, the legislation of the US, England, and France directly affects the work of corporate security systems. Examples include the law on GDPR (General Data Protection Regulation) and the Loi SAPIN II Law. When I said that corporate security is everything, it was no exaggeration.

The realization of this fact by the business community under the influence of all the above-mentioned reasons has become the main factor for the rapid development of corporate security in the country.

Either you change, or you don't survive.

UJBL Corporate governance is frequently referred to as an essential and very sensitive field for security of business. Would you agree?

S. P.: Yes, I do. I would even assert that business structures that ignore the need to study, implement, and continuously develop the best practices of corporate governance may sooner or later cease their activities or be lost to their owners.

We can clearly see how in the era of the so-called intellectual corporate raiding in 2000-2008, companies with a weak corporate governance system most often became the target of raider attacks, which, in the first place, became possible due to errors in corporate governance.

For example, many had very poor-quality charters, which led to the possibility of various manipulations to seize leading positions or hold meetings of shareholders with numerous violations; there was no contact with minority shareholders, which allowed for the purchase of significant share stakes with subsequent attacks on joint-stock companies. The owners of companies often did not pay attention to the concentration of the majority stake or distributed the blocks among the members of the Board of Directors on the basis of heads of agreement, which subsequently led to the loss of business. It was a common practice to bribe the director general to withdraw assets from the company or sign fictitious debt obligations owed to the company, etc.

S. S.: The current trend in large corporate structures is fraud, embezzlement, abuse of office, and corruption — white-collar crimes.

In my experience, every company that begins to improve its system of corporate governance arrives at the idea of building a corporate security system. These are two evolutionarily inseparable processes.

UJBL Do you see increased demand for corporate security audits?

S. P.: Increased demand for corporate security audits can only occur in a business community that knows what it is, needs an audit, and is willing to pay money for safety. Since our business community has not yet reached this level of development, there is certainly no increased demand.

There is usual demand for an unusual service. A corporate security audit is a relatively new proposal. It should be understood that this is not an audit of busi-

ness security, which is a highly specialized kind of activity within the company. The methods of corporate security audit, as well as experience of conducting such audits in Ukraine, are only developing.

The fact that a corporate security audit is a new service can be clearly seen in the Head of Corporate Security course. Many participants on this course, who are the leaders of the country's largest private security services, stated frankly that they did not view the security service operation as part of the corporate security system with this level of authority and penetration into all business management processes, up to participation in the Supervisory Board of the company.

Such an audit lasts from three to six months and is expensive. Customers are, as a rule, large companies with one or more owners who find it important to have a higher level of security and control.

As issues of business security, safe succession, and security of consistency of corporate governance become increasingly important in our country, and the situation in the country stimulates the business community to deal with it, I find the number of orders for corporate security audit quite satisfactory for today.

From next February, we are going to expand our practice of corporate security and criminal defense in anticipation of higher demand for these services.

UJBL What are the main red flags in this audit that companies should thoroughly revise?

S. P.: I think companies must thoroughly study the entire corporate security audit report.

The report, as a rule, describes and assesses achievements and failures, including corporate governance issues affecting business security. Together with the Association of Corporate Security Professionals (APKBU), we have developed a GSA (Global Security Assessment) software package based on international safety standards and adapted to the Ukrainian market. Using various data on certain areas of security and the company's activities, we get a graphical representation of the level of maturity of business security. We also identify high-risk areas for each type of security and recommendations from specialists for their elimination.

The complex works on thirty separate types and directions of security and separately on corporate management and personnel integrity. Based on the re-

sults of the audit, the customer receives a memorandum proposing analysis of the existing security system, including:

- Identification of weak and exposed areas in the security system;
- Analysis of organizational and distributional documentation;
- Testing of security systems for vulnerability;
- IT security audit;
- Identification, analysis, and assessment of basic risks;
- Analysis of the state of corporate governance and interaction between business units in terms of ensuring business security;
- Analysis of existing security and control policies;
- Identification of unreliable and disloyal employees, as well as professional suitability check;
- Evaluation of the security of the main business processes;
- Analysis of the level of access of employees to material valuables and information;
- Identification of types of economic risks and their likelihood;
- Development of the structure of security services and recommendations for its creation, inclusion in corporate management processes, and control.

GSA allows for a more detailed analysis than the standard audits and questionnaires of various types that exist today. In 100% of cases, the corporate security audit unpleasantly surprised the owners in terms of identifying risks in their company of which they were not previously aware.

UJBL Do you think that there is a standalone corporate security market in Ukraine?

S. P.: There is a security market. It is chaotic, unstructured and without normal standards of professionalism, but it does exist. Unfortunately, during the twenty-seven years of Ukraine's independence, professional private security associations, federations, and unions failed to reach a sufficient level of development to unite the entire the Ukrainian market.

There are no laws that would provide impetus for the civilized development of the market: such laws as *On Civilian Circulation of Weapons*, *On Private Detective (Investigation) Activity*, *On Trade Secrets and Confidential Information*, *On Private Military Companies*, and other laws regulating the private security market.

As for the corporate security market, it practically does not exist. This is due to the small number of consumers of this service, the lack of a pool of potential participants in the market, and their lack of a clear understanding as to what corporate security is.

Corporate security is a new profession. At the same time, it is a security direction able to unify corporate governance, security, and a number of other areas and opportunities that we have discussed previously.

The corporate security market is going to absorb all the individual markets and professions in this field over the next 10 years. I think I will be able to respond positively to your question no earlier than 2028.

UJBL If so, what are the prospects for its development?

S. P.: All market participants will have a lot of interesting and difficult work to do to make the market succeed.

When we and our colleagues created APKBU in 2014, we set the Association several tasks: the promotion of corporate security in the business environment, the training of business representatives and our market colleagues in corporate security, and adopting the best world practices and standards in the field of security in Ukraine. As part of the promotion and training of the business environment, we hold roundtable discussions, seminars, and the annual Corporate Security Conference. The conference has become a milestone event in the corporate security sphere in Ukraine. It attracts 350 people, including representatives of foreign embassy delegations. The speakers include high-ranking state officials, heads of big business and corporate security. We are set to hold the third Conference this year.

S. S.: To train the market, we have launched a specialized course called the Head of Corporate Security. One in every four people who applied was accepted, which indicated high demand for corporate security knowledge. We contemplate in the next five years creating a Corporate Security faculty with one of the country's leading universities, and opening an Academy of Corporate Security to gather all security professions under one wing. We hope that in future Ukraine will take its rightful place in the global private and corporate security market.

END 