JEL Classification: M10; M12; M15; M31 **DOI**: https://doi.org/10.31521/modecon.V21(2020)-03

Budnyk Liudmyla, PhD (Economics), Associate Professor of the Department of Security, Law Enforcement and Financial Investigations, Ternopil National Economic University, Ternopil, Ukraine

ORCID ID: 0000-0002-1393-9354
e-mail: lydabydnik@gmail.com

Blazhei Iryna, PhD (Economics), Lecturer of the Department of International Economic Relations, Ternopil National Economic University, Ternopil, Ukraine

ORCID ID: 0000-0002-0649-4991
e-mail: i.blazhey@gmail.com

External and Internal Marketing of the Information Security Company

Abstract. Introduction. *Security issues are increasingly becoming the focus of top management. The relevance of this topic is that the security of commercial and financial information, the loss of which leads to financial and reputational risks, is becoming more significant. An information security strategy should be closely integrated into the overall corporate business program. Thus, the number of potential clients of the information security companies continues to grow steadily.*

Purpose. *The purpose of this article is to identify the most effective tools for external and internal marketing in order to strengthen the competitive position of the information security company.*

Results. *As a result of the research, the most common information security problems faced by enterprises were considered, and on this basis the company's marketing strategies for information security were highlighted. The most effective tools of external marketing, taking into account the specifics of the enterprise, are proposed, which allows to increase consumer awareness of the proposed product or service, as well as to improve the level of competitiveness. The principles of internal marketing are highlighted, using which the company will be able to achieve its marketing goals in a shorter period of time, compared with the classical marketing strategy. The importance of using internal marketing to establish a positive corporate image of the information security company, as well as to create a system of employee motivation, has been proved.*

Conclusions. *In the management of the information security company, it is important to take into account its specifics, because the offerd products are not well known, and their importance for consumers is not heavily advertised. The use of external and internal marketing will allow the information security company to achieve market goals faster, increase its recognition and, most importantly, explain the value of information security for effective business management.*

Keywords: *consumer behavior; external marketing; information security; internal marketing; management; marketing strategy; human resources management.*

УДК 339.13 (004)

Будник Л. А., кандидат економічних наук, доцент кафедри безпеки, правоохоронної діяльності та фінансових розслідувань, Тернопільський національний економічний університет, м. Тернопіль, Україна

Блажей І. О., кандидат економічних наук, викладач кафедри міжнародних економічних відносин, Тернопільський національний економічний університет, м. Тернопіль, Україна

Зовнішній та внутрішній маркетинг компанії з забезпечення інформаційної безпеки

Анотація. *На сьогодні створення системи інформаційної безпеки є одним з першочергових завдань кожного підприємства, направлених на запобігання ризиків, пов'язаних з такими загрозами як витік або крадіжка закритої інформації, порушення авторських прав. Саме прийняття превентивних заходів з метою забезпечення конфіденційності та цілісності інформації є ефективним підходом до інформаційної безпеки. Водночас компаніям з забезпечення інформаційної безпеки складно зайняти ключові позиції на ринку інформаційних технологій, адже керівництво інших підприємств не завжди усвідомлює, наскільки важливим є даний продукт чи сервіс.*

Метою статті є виокремлення найбільш ефективних інструментів зовнішнього та внутрішнього маркетингу задля посилення конкурентних позицій компанії з інформаційної безпеки.

У статті досліджено підходи до управління компанією з забезпечення інформаційної безпеки, які передбачають збільшення кількості продаж за рахунок використання інструментів зовнішнього та внутрішнього маркетингу. Розглянуто найбільш поширені проблеми інформаційної безпеки, з якими стикаються підприємства, на цій основі виокремлено товарні маркетингові стратегії компанії з забезпечення інформаційної безпеки. Запропоновано найбільш ефективні інструменти зовнішнього маркетингу з врахуванням специфіки підприємства, що дозволяє підвищити обізнаність споживачів про запропонований продукт чи сервіс, а також покращити рівень конкурентоспроможності. Виокремлено принципи внутрішнього маркетингу, використовуючи які, підприємство зможе досягти поставлених маркетингових цілей за менший проміжок часу у порівнянні з класичною маркетинговою стратегією. Доведено значущість використання внутрішнього маркетингу для формування позитивного корпоративного іміджу компанії з забезпечення інформаційної безпеки, а також для створення системи мотивації працівників.

Стаття надійшла до редакції: 20.06.2020
Received: 20 June 2020

Маркетинг допомагає створити умови для підвищення обізнаності про продукти інформаційної безпеки. Послуги можуть бути якісними та технічно досконалими, але саме маркетинг забезпечить необхідну рекламу та сформує потреби клієнтів, у той час як комплексне застосування внутрішнього та зовнішнього маркетингу дозволить створити цілісне зображення компанії та створити необхідний попит на продукти інформаційної безпеки.

Ключові слова: *внутрішній маркетинг; інформаційна безпека; захист інформації; зовнішній маркетинг; маркетингова стратегія; менеджмент; поведінка споживачів; управління персоналом..*

Formulation of the problem. Usually, information security is understood as the security of information and the entire company from deliberate or accidental actions leading to damage. The ensuring of information security should be aimed primarily at preventing risks, and not at eliminating their consequences. It is the adoption of preventive measures to ensure confidentiality, integrity, and also the availability of information and is the most appropriate approach to creating an information security system. The taking of precautionary measures to ensure confidentiality, integrity and accessibility of information is the most appropriate approach to creating an information security system.

Any leakage of information can lead to serious problems for the company – from significant financial losses to complete liquidation. Of course, the problem of leaks did not appear today – an industrial espionage and a luring of qualified specialists existed even before the era of computerization. But it was the appearance of PCs and Internet that led to new methods of obtaining information illegally.

Most often, financial documents, technological and design developments, logins and passwords for entering the network of organizations leak from companies. But a serious damage can also be caused by the leak of employees' personal data. This is especially true for Western countries, where lawsuits due to such leaks often lead to huge fines, after which companies suffer serious losses.

It also happens that a leak harms a company several months or years after it occurs, falling into the hands of competitors or journalists. That is why protection should be comprehensive. We should not divide information into very important and less important. Everything related to the activities of the company and not intended for publication should remain within the company and be protected from threats.

This explains the need for an in-depth study of the management of information security companies, for the sake of their active involvement in the market.

Analysis of recent research and publications. For several decades, especially in the second half of the 20th century, information security has been the subject of scientific research. Since then, Western scholars have continued to be interested in issues arising in the field of information conflict and information security.

From a large number of theoretical studies of information security problems, we highlight the work of D. Alberts, J. Hall, K. Haufe, G. Sabatini, R. Schultz, S. Park, K. Lee, etc., who studied various aspects of the impact of information on economic, political, cultural and military processes in international relations.

The general subject of studies addressing the problems of using information technology in the scientific literature is presented by the technological and humanitarian areas of solving information security problems. In contrast to the technological approach that develops the software and hardware side of the information security process, the humanitarian one considers information security as an interdisciplinary field of scientific knowledge, highlighting the legal, sociological and psychological aspects of this phenomenon.

The interdisciplinary problems of information security are the subject of research by M. Dmytrenko, S. Makarenko, S. Severina, S. Skulysh, V. Stepanov.

From the analysis of the available literature it follows that the problems of the use of information technology have been sufficiently studied. At the same time, it is important to note that there are actually very few special researches, which cover the managerial aspects of information security.

Formulation of research goals. The purpose of this article is to identify the most effective tools for external and internal marketing in order to strengthen the competitive position of the information security company.

Outline of the main research material. There are a number of scenarios that implement internal threats. Each of these scenarios takes into account the specific purpose of illegal actions and the technical means of achieving it.

1. Disclosure of confidential information. This type of threat involves the disclosure of information constituting a trade secret by sending it by e-mail, via the Internet (chat, forum, etc.), using instant messaging tools, copying information to portable media or by printing data. To detect the fact of disclosure of confidential information, different companies offer the interception of mail, intranet and Web traffic with subsequent analysis by various filtering methods, including content analysis [1].

2. Bypassing means of protection against the disclosure of confidential information. It can be achieved using various data transformations, for example, encryption, archiving with great nesting depth, conversion to graphic format or rare text formats, encoding changes, use of unknown software or communication in a foreign language unfamiliar to most company employees. Protection systems against confidential data leaks deal with such actions, supporting a variety of file formats and responding to any suspicious actions (unknown file format, encryption, etc.).

3. Theft of confidential information. Illegal access to information is possible when it is transmitted through a regular connection (without encryption) – by breaking into a corporate network; if the data is located in places

accessible to strangers or employees who do not have the appropriate rights; if an outsider has the ability to read from the monitor screen; if an outsider has the access to printed materials, portable media, or computers.

4. Infringement of copyrights. As a part of the threat of copyright infringement, it is possible to copy portions of documents of one author to documents of another author (as well as mail messages, Web forms, etc.); individual encryption of documents, in which the company is deprived of the opportunity to work with the document after the dismissal or transfer of an employee or in the case of a password loss; use of materials published on the Internet without processing in their documents; the use of multimedia files (graphics, audio and video), software and other information objects protected by copyright; falsification of the data of the addressee or sender in order to discredit his good name or discredit the company [2].

5. Inappropriate use of resources. Misuse of resources means visiting sites of a general and entertaining orientation (not related to the performance of official duties) during working hours; loading, storage and use of multimedia files and entertainment software during business hours; the use of rude, incorrect vocabulary in the conduct of business correspondence; downloading, viewing and distribution of materials for adults, as well as materials containing Nazi symbols, agitation or other illegal materials; using company resources to send advertising information, spam, or personal information, including information about employees, social security numbers, credit cards, etc [3].

Information security should be carried out comprehensively, in several directions at once. The more methods are used, the less likely there will be threats and leaks, and the more stable will be the company's position in the market.

Information security marketing has its own specifics, which depends on the type of company providing services. Marketing techniques used in the IT field are constantly expanding, new tools and technologies are emerging, and traditional techniques are improving. A large amount of information goes online, which entails the movement of Internet consumers. Seminars give way to webinars, mailing lists give way to electronic ones, and a website becomes an indispensable attribute of a company's business.

The site for the informational security company is a business card, since it demonstrates to the client the capabilities of the company. It is important for the consumer that the company page looks attractive, and is not difficult to find. Therefore, the website of an informational security company requires effective promotion in leading search engines. Competent SEO-optimization of the site helps to occupy high positions in search results to attract visitors to the web-resource. Also for this purpose, company can conduct site promotion using contextual advertising, banners and social networks [4].

Furthermore, trial programs can serve as s good opportunity to demonstrate the goods and services of a company engaged in the development of informational security software. This marketing tool involves demonstrating a product or service to the desired target audience. The purpose of this demonstration is to show those product features that look favorably compared to competitive offers. The informational security company presents the product to the consumer, offering him to test the product. This clearly convinces the consumer to purchase this product, as it demonstrates the openness of the company, and also provides an opportunity to understand what advantage this advertised product has. More effective are user test programs. Company can offer the target group a version of the product that is limited in capabilities or in validity [5].

A new and effective tool today, which can be used both to develop the image of the company, and to promote various products and services, are promotional videos. If the video is interesting and creative, then it invariably catches the attention of a viewer. It is also true, that their manufacture requires considerable financial resources and the involvement of a creative team.

Other marketing tools are business cases. Placing on the enterprise's website information about a specific problem or task that confronted it before the implementation of the project, alternative options, the reasons for choosing this solution and the results achieved, will additionally attract potential consumers. They will be able to draw an analogy between the described situation and their own. Often, it is business cases that make costumers choose in favor of certain products. Depending on the tasks to be solved, such materials can be oriented both to managers and specialists. In the future, cases can be used as independent marketing materials, included in booklets, and form the basis for industry publications. It should be noted that in some cases it is quite difficult to motivate consumers to participate in the preparation of the case and the coordination of materials. For obvious reasons, companies are extremely reluctant to admit the installing of various information security systems, antivirus software, etc.

However, we should not forget that if marketing activity does not attract attention, then it will not work. And it doesn't matter which tool the company uses, it matters how much it understands its customer.

It is possible to allocate such modern marketing strategies in the field of informational security:

– Development only. The company creates the product and sells it as whole or as a part (licensing) to other companies. This strategy is justified when the consumer market is limited or the promotion of the product by the enterprise is impossible due to lack of certain resources or lack of access to marketing channels;

– Specialization. The company specializes in only one area of activity, while providing a full range of services. Specialization strategies are not effective in the long run, primarily due to rapid changes in technology. Specialization strategies are used by companies at the stage of their development, later these companies diversify to increase competitiveness. Business in the field of information security is characterized by the acquisition of some companies by others, and the separation of some major divisions into separate companies. In case of acquisition of another company, the company gets certain competitive advantages and access to new technologies, and, most importantly – to customers of the company it acquired (in case the purpose of acquisition was not technology), i.e. gets access to marketing channels. The separation of units is characteristic of multinational corporations. In the case when a division develops its own brand, then two options are possible: either competing between its own brands to increase market share, or generating large profits [6];

– Narrow specialization. The company is engaged in only one type of activity, without providing a full range of services.

– Diversification. The company specializes in providing comprehensive services to a specific segment of end-users and provides a full cycle of services in each direction. The specificity of this strategy is the need for the company to constantly expand the range to ensure competitiveness.

– Wide diversification. The company is engaged not only in servicing of end-users, but also in distribution.

Modern marketing strategies of enterprises in the field of information security involve the management of marketing channels. The specificity of the industry is the lack of time to build their own marketing channels and correct marketing errors. It is the rapid development of the industry that encourages companies to operate in this market to build relationships with consumers based on their needs and capabilities.

With each passing day, the Internet is playing an increasingly important role as both a marketing channel and a distribution channel. This is especially true of information security software. With the help of the Internet, the consumer can quickly get a software product directly from the developer, which in turn is a source of additional revenue for the latter. It should be noted that the Internet has given impetus to the development of software outsourcing – software rental over the Internet.

Internal marketing is a personnel-oriented management activity to ensure the effective implementation of tasks by employees to achieve the organization’s intended marketing goals. It is possible to develop an attractive marketing strategy aimed at external consumers, however, the final result will substantially depend on the quality of staff work to implement it. Therefore, internal marketing is defined as a focused activity to overcome staff resistance to organizational changes, by its motivation and integration in order to effectively implement company strategies [7].

The philosophy of internal marketing is that the organization-staff relationship is built on the same basis as the organization-client. The company offers a special product – a position in the company with its specific rights and obligations. The employee buys this product, paying it with his labor. Accordingly, the focus on the client, the external consumer, the basis of the traditional understanding of marketing, is complemented by the orientation on the “internal consumer” – the employee.

The principles of internal marketing include:

– focus on needs of staff;

– motivation of all company personnel to meet the needs of external consumers;

– use of traditional marketing methods within the organization;

– cross-functional cooperation of all divisions, active interaction of personnel with managers, clients, other stakeholders;

– willingness to change.

One of the most significant areas of the implementation of the internal marketing plan in the information security company is to provide ongoing support from managers at all levels. The primary target segment of internal marketing is top management. The success or failure of internal marketing largely depends on how much it will be possible to arrange the organization’s senior staff, which will subsequently be reflected in the attitude and actions of all employees. It is known that the implementation of changes most often occurs from top to bottom: top managers form the vision and mission of the organization; then middle managers embody these ideas in their daily activities; finally, when performing their work, all employees begin to think in the light of new goals and values common to the whole company and understandable to everyone [8].

Training primarily concerns personnel who are in direct contact with consumers, but other employees should not be left aside. It is important that each employee is included in the implementation of all stages of internal marketing; this will ensure its better understanding, acceptance and successful implementation. Widely used in practice is the scenario method of training (the so-called role-playing games), when each employee is given “scenarios” of his behavior when interacting with consumers (including key phrases for starting, developing and ending a conversation). The purpose of the training is to develop the skills of personnel to apply existing knowledge and experience not only to meet current needs, but also to build long-term, mutually beneficial relationships with consumers.

Training helps to ensure that the thinking and actions of staff are consistent with the direction of development of the organization as a whole. For this, for example, employee involvement in the organizational planning process may be practiced [9]. This allows, firstly, to exchange information, identify problems and possible solutions to them jointly by employees and managers of the organization; secondly, to bring to employees an understanding of the need to better meet customer needs and win competition; thirdly, to ensure the coherence of the actions of all personnel of the organization.

Practice shows that training programs alone are not enough to achieve success in the implementation of internal marketing. The third area of communication includes providing wide opportunities for receiving and exchanging information between employees of all levels, both during training and in the implementation of internal marketing in the organization. Mid-level managers can use slides, video tapes, printed materials, information on stands and at a company's website to popularize among employees the main provisions of the organization's mission; to illuminate the methods expected of employees and to fulfill their responsibilities and their contribution to the achievement of the organization's common goal [10].

Personnel management includes recruiting and selecting employees suitable for the organization; designing their training and development; measuring and managing their performance; assessment, payment and remuneration; career planning of employees. These components of personnel management must be coordinated with other internal marketing activities in order to ensure consistency and continuity of their implementation.

Customer orientation is aimed at informing staff about the products or services provided by the organization. To do this, advertising campaigns are conducted, brochures are distributed that differ from those prepared for external consumers in that they often refer to the main provisions of the organization's mission (how they are embodied in the work of each unit of the organization and how they are reflected in its final products). Such events allow employees to express their ideas, ask questions, give comments on the organization's products or services for external consumers. Thus, the relationship of internal and external marketing is ensured.

Conclusions. Information security is one of the important tasks of any enterprise, while marketing helps to create conditions for promoting awareness of information security products. Services can be of a high quality and technically perfect, but it is marketing that will provide the necessary publicity and shape the needs of customers. Such a strategy, combined with configured communications, will to some extent be able to compensate for the lack of synchronization of business processes and information security of Ukrainian companies.

It is generally accepted that the role of marketing is only to profitably sell the product or service to external consumers. In fact, the primary task of marketing very often becomes the "sale" of the company's goods or services to inner consumers – organization staff. External marketing can achieve its goals only if the employees have a clear idea and emotional commitment to what constitutes the company's commercial offer.

References:

1. Surmiak, A. (2019). Should we Maintain or Break Confidentiality? The Choices Made by Social Researchers in the Context of Law Violation and Harm. *Journal of Academic Ethics*. doi: https://doi.org/10.1007/s10805-019-09336-2.
2. Reddy, A. & Aswath, L. (2016). Understanding Copyright Laws: Infringement, Protection and Exceptions. *International Journal of Research in Library Science,* 2 (1), 48-53.
3. Torsen, M. & Anderson, J. (2010). Intellectual property and the safeguarding of traditional cultures. Legal Issues and Practical Options for Museums, Libraries and Archives. World Intellectual Property Organization (WIPO), 126 p. Retrieved from https://www.wipo.int/edocs/pubdocs/en/tk/1023/wipo_pub_1023.pdf.
4. Root, A. (2020). Cyber security marketing tactics that actually work. SevenAtoms. Retrieved from https://www.sevenatoms.com/blog/cyber-security-marketing-tactics-that-actually-works.
5. Datta, H., Fouber, B. & van Heerde, H (2015). The impact of free-trial acquisition on customer usage, retention, and lifetime value. *Journal of Marketing Research,* LII, 217-234.
6. Insights (2017). How to Create a Marketing Strategy for Information Technology Services. Retrieved from https://www.ironpaper.com/webintel/articles/marketing-strategy-information-technology/
7. Bohnenberger, M. C., Schmidt, S., Damacena, C. & Francisco, J. (2019). Internal marketing: a model for implementation and development. *Dimensión Empresarial*, 17(1), 7-22. doi: http://dx.doi.org/10.15665/dem.v17i1.1657.
8. Akbari, M., Chajnani, M.H. & Aletaha, S. H. (2019). Internal Marketing and the Internal Customers' Citizenship Behavior in Higher Education. *International Journal of Schooling*, 1(3), 15-28. doi: http://dx.doi.org/10.22034/ijsc.2019.202676.1018.
9. Mohanty, A & Mishra. B. (2019). Internal marketing mix and employee satisfaction in service industry – a literature review. *International Journal of Business Marketing and Managemen,* 4 (7), 5-16.
10. Raziq, A. & Maulabakhsh, R. (2015). Impact of working environment on job satisfaction. *Economics and Finance*, 23, 717-725.