In “regulated civilian markets” for advanced cybersecurity, firms develop innovative solutions for non-military industries. (Medicine and finance are examples of these industries.) These solutions can be applied in a global market.

Croatian cybersecurity firms can enter this strategic segment by finding unserved market demands. They may arise from new regulatory requirements, shifting customer needs, or new cyber threats.
Industry Snapshot

Cybersecurity includes activities focused on protecting computers, networks, software, and data from unauthorized or unintended access. Cybersecurity preserves the availability and integrity of information and communication networks and infrastructure.

By 2020, buyers will spend EUR 582 billion on cybersecurity. Of this total, buyers will spend EUR 343 billion on securing PCs, EUR 153 billion on securing “internet of things” (IoT) devices, and EUR 100 billion on securing mobile devices.

The Croatian IT sector had more than EUR 1.9 billion of turnover in 2016. Some 3,800 companies are in the Croatian IT sector. They employ over 19,500 people.

The IT sector is one of the main drivers of economic and social development in Croatia. IT firms achieved impressive growth in employees, exports, and revenues between 2011 and 2016 compared with other industries in Croatia.

The IT sector is one of the main drivers of economic and social development in Croatia.
Cybersecurity firms supply three major types of services:

- **Monitored security services**—supplying outsourced cybersecurity services. Examples include security audits, digital forensics, round-the-clock monitoring and management of intrusion detection systems and firewalls, training services, and response and remediation services.

- **Off-the-shelf integration services**—selling and integrating third-party solutions with little or no innovative components or development. Examples include installing antivirus programs, setting up backup systems, configuring firewalls, and selling disaster recovery tools.

- **Solutions development services**—creating newly-developed products or services with innovative components. The term “solutions” here refers to either products or services—or any combination of them—that solve cybersecurity problems. Firms patent and protect their novel solutions, raising barriers to entry.

There are three main markets for cybersecurity solutions:

- **The military market.** This market is not addressed in the analysis, as per World Bank policy.

- **The unregulated civilian market** refers to individuals and unregulated corporate sector purchasers that require cybersecurity solutions and products.

- **The regulated civilian market** refers to advanced buyers of cybersecurity solutions and products that come from highly regulated corporate or public sectors. In these industries, regulatory requirements are continually evolving, and standards are highest.
The “regulated civilian solutions” is a growth opportunity for Croatian cybersecurity firms. It combines two attractive opportunities: solutions development (i.e. the creation of customized or bespoke services); and demand from regulated markets (i.e. advanced purchasers willing to spend more to comply with regulatory requirements).

The “regulated civilian solutions” strategic segment has several important characteristics:

- **Purchasing criteria are complex.** Buyers in the “regulated civilian solutions” strategic segment are looking for high-quality solutions customized to their specific needs.

- **Purchasers are sophisticated.** Buyers in the “regulated civilian solutions” strategic segment have advanced needs. They may need to manage sensitive data (financial and health care), run critical infrastructure (energy, utilities, and telecommunications), or protect lives (automotive and airspace). Buyers in this strategic segment are very aware of security needs and are the largest purchasers of cybersecurity products overall.

- **Purchasers will pay to decrease risk.** Willingness to pay for cybersecurity solutions derives from the economic incentive to minimize duration and errors in regulatory compliance processes to reduce the risk of sanctions. Purchasers in the “regulated civilian solutions” strategic segment also want to minimize reputational risks that might result from security breaches.

*Managing sensitive data (financial and health care), running critical infrastructure (energy, utilities, and telecommunications), and protecting lives (automotive and airspace)*
CROATIA: CYBERSECURITY

MAKING CROATIA COMPETITIVE

Where Is the Value Chain Weak?

Croatian companies’ ability to thrive in the emerging “regulated civilian solutions” strategic segment depends on their ability to evolve their products to meet buyers’ demands. Croatia lags in several areas along the value chain:

- Most Croatian cybersecurity companies are system integrators. They sell and integrate imported pre-made products and solutions made by international companies such as Cisco, Symantec, IBM, Microsoft, and Oracle.
- Croatian companies dealing with cybersecurity are scarce. Only a few have research and development (R&D) capacities to develop their own products.
- Firms struggle with retaining top talent. Some of the best professionals are migrating to countries offering better pay and working conditions.
- Research, development, and innovation are unsatisfactory. Croatia’s IT firms lack substantial R&D and innovation activities. Croatia, with only 3.2 European patent applications per million inhabitants, was 41st out of 48 ranked countries in 2016.
- Capacity in both certification and accreditation bodies needs improvement. Because buyers in the “regulated citizen solutions” strategic segment are subject to regulation, certification and supervising authorities play important roles.

Croatian cybersecurity IT companies are system integrators.

Growth rates of Croatian Industries, 2011–2016 (Revenues, Exports, and Employees)

Areas for Reform

Certain aspects of the industry ecosystem limit Croatia’s competitiveness in the emerging “regulated civilian solutions” strategic segments.

Demand Conditions

Demand in Croatia for high-complexity customized cybersecurity solutions is low. However, due to existing and incoming regulation (GDPR, NIS Directive, etc) and rising awareness among buyers, domestic demand is expected to increase substantially.

Exports are low compared to international competitors. Croatia needs more focused export strategies. High-value export opportunities are in neighboring countries, the western EU countries, and the United States.

Factor Conditions

Technology infrastructure is below par. In 2017, Croatia ranked 24 out of the 28 EU member states in terms of progress toward societal digitization, according to the DESI index.

Labor productivity is low. From 2000 to 2014, productivity increased by only 20 percent while real wages increased by over 70 percent. This gives cause for concern about the long-term cost-competitiveness of the Croatian workforce.

Finding and retaining top talent is difficult. Croatia does not have enough educated, highly skilled workers to compete in the IT industries. In 2016, only 2.7 percent of the workforce in Croatia were information and communications technology (ICT) specialists. Additionally, good software and systems engineers can move to other companies abroad for much higher net wages.

Access to finance is limited. Financial institutions do not offer the capital for R&D investment that firms in this segment need. There is no smart venture capital that could guide young entrepreneurs and open new markets for more mature companies.

Vocational education and training could be better targeted. Comprehensive, specialized courses and programs in cybersecurity are lacking.

Croatia’s innovation capacity is limited. The Croatian innovation system is inefficient, complex, and fragmented.

Strategy, Structure, and Rivalry

Croatian cybersecurity companies have limited negotiating power. Croatia’s cybersecurity firms are generally small- and medium-sized enterprises (SMEs). Because their buyers are larger corporations and the public sector, they have limited negotiating power.

Croatian IT companies face fierce global competition. Eastern European countries have lower prices and larger volumes.

Related and Supporting Industries

There is no systematic cooperation on specific projects between the private sector and academia. Private contacts and individual efforts are behind most collaboration today.

Scientific research in Croatia often does not follow the needs of the business sector. Firms need to collaborate more with research agents and other stakeholders.

Collaboration between companies working in the IT sector is low. Competitiveness clusters need to improve cooperation and exchange of valuable information about everyday business operations (especially export activities). Several associations represent the industry’s interests. However, their efforts are uncoordinated and are relatively passive.
Government

Croatia’s innovation policies can move further towards commercialization. Policymakers can improve support programs for innovation aimed at commercialization.

Croatia taxes skilled labor unfavorably. Croatia has higher taxes for skilled labor than other countries in Central and Eastern Europe (for example, Romania or Bulgaria). Many additional costs (such as taxation of travel expenses for longer-term assignments and taxation of daily rates over a certain threshold) also make labor more expensive for Croatian companies.

Croatian companies are subject to double taxation in some of the countries that are the biggest buyers of cybersecurity products. Croatia is the only EU member that has not signed a Double Taxation Treaty (DTT) with the United States, the largest global market for cybersecurity products. Croatia has also not signed DTTs with many other developed countries and economies. Croatian companies are therefore at a competitive disadvantage, since they will be taxed in Croatian and in their export destination.

Croatia lacks specific incentives for R&D or exports of software products. Croatia faces stiff competition from other countries that strategically support the cybersecurity industry. Most neighboring countries offer incentives for creating and growing local IT companies. There are only a few such incentives in Croatia.
Recommendations

Croatia could improve its position in the emerging “regulated civilian solutions” strategic segment by:

1. Creating a cybersecurity ‘Digital Innovation Hub’ (DIH). Setting up a DIH for cybersecurity in Croatia could provide a leg up for an industry at the leading edge of disruptive change focused on commercializing innovative products. The Ministry of Economy Entrepreneurship and Crafts (MoEEC), the Ministry of Science and Education and other line ministries could implement this recommendation.

   Estimated timeframe: 3 years.

2. Skills development. The training would cover cutting-edge technologies, products, and services developed elsewhere. MoEEC could contract this program to relevant government agencies as a technical assistance program.

   Estimated timeframe: includes short- (1 year) and long-term (10 year) programs.

3. Improving the business environment. Croatia’s business environment can be enhanced to encourage Croatian companies to transition toward new attractive opportunities in the cybersecurity sector. There are three top priorities. The first is facilitating mobility between academia and the private and public sectors. The second is reducing business environment constraints on IT and cybersecurity firms, particularly by signing treaties to prevent double taxation. The third is paying special attention to cybersecurity as a priority segment for investment promotion and policy efforts. MoEEC and other relevant agencies could implement these regulatory reforms through public institutions and government agencies.

   Estimated timeframe: 3 years.

NOTE
This report is a product of the staff of the World Bank Group. The findings, interpretations, and conclusions expressed in the report do not necessarily reflect the views of The World Bank Group, its Board of Executive Directors, or the governments they represent. The World Bank Group does not guarantee the accuracy of the data included in this work, which is drawn from multiple external sources. Nothing herein shall constitute, or be considered to be, a limitation upon or waiver of the privileges and immunities of The World Bank Group, all of which are specifically reserved.