Revising Cybersecurity Skills for Enterprises

Cyberspace is a virtual environment. Today, it does not matter which device is used for connecting to the Internet. Millions of users are there—in that virtual place—conducting day-to-day activities such as communicating, shopping, paying bills, searching for information, reading news, doing business, and controlling or managing something.

Cybersecurity is the ability to protect or defend the use of cyberspace from cyberattacks and is defined as the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

MAIN CHALLENGES FOR CYBERSECURITY
The main challenges faced by governments attempting to enhance their cybersecurity capability and, by doing so, ensuring reliable and properly protected information resources are:
- The increased importance of the national coordination of information and communications technology (ICT)
- Cooperation between the public and private sectors
- International cooperation
- Reinforced incident response
- Effective crime control
- Critical infrastructure protection

The development of democracy and social networks has expanded the virtual environment and turned it into an effective collaborative platform for municipalities, governments and politicians, as well as criminals who do not respect national borders. These criminals are called by different names, based on their motivations and competencies, including terrorists, hackers and other attackers.

The positive impact of this virtual world on democratic processes, driven by active participation of the population, is indisputable. It includes education possibilities and information exchange using cyberspace. However, the dark side of it cannot be ignored. Data thieves are professional criminals deliberately trying to steal resources and information utilizing lack of competence by users and sometimes even those who should protect the users.

The UK report Cyber Security Skills: Business Perspectives and Government’s Next Steps makes clear that having the skills and capabilities to manage cyberrisk effectively can reduce the financial cost to a business from cybercrime, and it can also increase consumer confidence, providing that business with a competitive edge. As businesses increasingly take steps to protect themselves from cyberattacks, demand for cybersecurity products and services will continue to increase, providing growth opportunities for the organizations that supply them. A highly skilled workforce will enable cybersuppliers to derive maximum benefit from these opportunities.

Cyberthreats have the power to drive up costs and affect revenue for companies, making them similar to any other financial risk. What organizations need are practical tools to mitigate this risk. Larry Clinton, Internet Security Alliance (ISA) president, said, “We need to connect the dots between the operational issues and the strategic issues which is what businesses focus on.”

PEOPLE AND SKILLS—PREPARING FOR CYBERSECURITY
Cybersecurity is a long-term trend in which information assurance, risk approach by default, and privacy by design indicate the evolution of information security and give broader understanding of cyberspace.

Cybersecurity skills are key elements of an organization’s preparedness to address cyberrisk.

Thus, in the field of cybersecurity, ability, knowledge and skills are essential for business survival in the virtual world and in the economy of tomorrow.

The recently released study, State of Cybersecurity: Implications for 2015 by ISACA and RSA, reveals that 82 percent of organizations expect to experience a cyberattack in 2015, yet more than one in three (35 percent) are unable to fill open cybersecurity positions.

The lack of cybersecurity professionals is a vulnerability in the three lines of defense.

The three lines of defense concept means collaboration and better understanding of how to
manage risk to an acceptable level. The first line of defense is responsible for day-to-day activities—monitoring and protecting information assets. The second line of defense is responsible for governing those tasks and ensuring that information assets have applicable monitoring, reporting and tracking; and the third line of defense is responsible for ensuring compliance.

In this case, soft skills for risk managers; auditors; process, information and system owners, including information security managers, are needed to resolve problems more creatively to assure the confidentiality, integrity, availability and accountability of an organization’s information assets.

Cybersecurity will continue to pose a serious risk, of which top management needs to be aware, measure and supervise continuously. This process should be a part of the company’s strategy, and top management plays a strategic role in implementing the cybersecurity culture.

The motivation of hackers ranges from individuals testing their skills to break into the US National Aeronautics and Space Administration (NASA) systems to well-organized criminal enterprises hacking for profit to intrusions sponsored by foreign intelligence services.9

The comparably small size of certain governments, for example, Latvia, to other European Union (EU) member-states combined with the small size of the companies operating in these smaller countries are two of the main challenges to developing and maintaining skilled cybersecurity resources to fight cybercrime, which, in fact, can be a well-organized, multinational business with strategy, processes and quality management, a dynamic infrastructure, robust cash flow, and highly-skilled professionals.

This situation is worsened by the job market in which leading security services companies aggressively cherry-pick cybersecurity specialists by offering lucrative compensation packages along with intensive training for skills development. Cybersecurity employees with years of faithful employment at small, regional banks, universities and state governments get employment offers they simply cannot refuse. Panic ensues at many organizations when they lose security professionals who, more or less, owned the organization’s informal incident detection and response processes.10

A better understanding cyberecosystem elements, their relationships and main performance drivers makes it possible to plan and develop effective cybersecurity readiness, even within the limited resources and capabilities of small enterprises.

Cyberdefense requires short-term and long-term solutions for cybersecurity professionals in obtaining knowledge in different dimensions, including:

• Cybersecurity for computing professionals (e.g., computer science, software engineering)
• Cybersecurity for society (policy creators and decision-makers)
• Cyberdefense for operations

To strengthen the security of information resources, proactive behavior is no longer sufficient to safeguard the critical resources in the organization. Organizations need to go further; they need to reengineer the behavior, attitudes and knowledge of all stakeholders, including those outside the organization (e.g., customers, suppliers).

It is obvious that all kinds of Internet users, regardless of their age, business area and confidence, should expand their knowledge.

This leads to the conclusion that the main drivers toward reasonable cybersecurity are human resources—the capabilities for which can be developed as follows:

• Establish new professions
• Develop education curriculum
• Reengineer security awareness programs
• Reengineer mind-sets

The mind-set of the cybersecurity professional is a very important factor in preventing, detecting and mitigating security breaches. Developing this way of thinking must be part of recruiting and educating cybersecurity professionals,11 recalling the similarity with opposite forces in which the mind-set of the hacker is the main advantage in distinguishing the good and not-so-good hacker.

The core competencies cybersecurity managers must possess include:

• Plan, organize, direct, control and evaluate the operations of cybersecurity management systems, formulating strategies, policies and plans, and security architecture taking into account the legal and ethical issues of cybersecurity.
• Plan, organize, control and continually evaluate risk management procedures.
• Direct and advise staff engaged in providing holistic information security management integration and establish security awareness training.
• Direct and control corporate governance and regulatory compliance procedures, incident handling, and management.
• Plan, administer and control security requirements for projects, contracts, equipment, services, inventory skills and competencies for related professionals.
• Accept the responsibility for processes associated with business contingency and disaster recovery planning.
• Prepare reports and briefs for management committees evaluating the cybersecurity ecosystem.

The Skills Framework for the Information Age (SFIA)\textsuperscript{12} is a logical, two-dimensional skills framework defined by areas of work on one axis and levels of responsibility on the other. It has been proven to be an effective resource that benefits businesses by facilitating all aspects of the management of capability in corporate and educational environments.\textsuperscript{13} Further, the US National Initiative for Cybersecurity Education (NICE) provides a common understanding of and lexicon for cybersecurity work, defined as the capabilities critical for successful job performance across cyberroles and the behaviors that exemplify the progressive levels of proficiency associated with these competencies.\textsuperscript{14}

PEOPLE, NOT TECHNOLOGY, ARE KEY ELEMENTS OF CYBERSECURITY

The 2013 (ISC)\textsuperscript{2} Global Information Security Workforce Study\textsuperscript{15} was conducted in 2012 through a web-based survey. The study’s objective was to gauge the opinions of information security professionals regarding trends and issues affecting their profession and careers. Designed to capture expansive viewpoints and produce statistically significant results, a total of 12,396 surveys of qualified information security professionals were collected.

With security staff viewed as critical in importance, it is equally important to understand the acuteness of need, organizations’ ability to fund staff expansion and improvement, and the sought-after attributes of information security professionals. When examining the sought-after attributes of information security professionals, it is not just the skills that are important. Confirmation of those skills and professionals’ engagement in peer groups are also essential.

The 2015 (ISC)\textsuperscript{2} Global Information Security Workforce Study respondents ranked success factors of professionals in order of importance as shown in figure 1.

Across the entire survey, broad understanding of the security field was on top in terms of importance, followed by communication skills; technical knowledge, awareness and understanding of the latest security threats round out the top four. While skill and knowledge building must never slow down—attackers, hackers and other cyberthreat actors certainly will not—information security professionals must also translate their risk management expertise into organization-wide leadership.

![Figure 1—Success Factors of Information Security Professionals (Important and Very Important)](image)

<table>
<thead>
<tr>
<th>Success Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broad understanding of the security field</td>
<td>92%</td>
</tr>
<tr>
<td>Communication skills</td>
<td>91%</td>
</tr>
<tr>
<td>Technical knowledge</td>
<td>88%</td>
</tr>
<tr>
<td>Awareness and understanding of the latest security threats</td>
<td>86%</td>
</tr>
<tr>
<td>Security policy formulation and application</td>
<td>75%</td>
</tr>
<tr>
<td>Leadership skills</td>
<td>68%</td>
</tr>
<tr>
<td>Business management skills</td>
<td>57%</td>
</tr>
<tr>
<td>Project management skills</td>
<td>55%</td>
</tr>
<tr>
<td>Legal knowledge</td>
<td>42%</td>
</tr>
</tbody>
</table>

Source: The 2013 (ISC)\textsuperscript{2} Global Information Security Workforce Study\textsuperscript{16}
CONCLUSION
When taking into account the aforementioned frameworks and the demand in the market for new cybersecurity professionals, it can be concluded that good technical knowledge of cybersecurity alone is not enough to establish effective cybersecurity and broader understanding of the business and human management principles. Strategic skills are equally important, especially in smaller organizations that cannot afford narrow specialization of their resources.

ENDNOTES
1 National Institute of Standards and Technology, NIST IR 7298 Revision 2, Glossary of Key Information Security Terms, USA, 2013
5 Ibid.
8 Ibid.
12 SFIA Foundation, Skills Framework for the Information Age, UK, www.sfia-online.org/
13 Ibid.
16 Ibid.