Arne Schönbohm took office as President of the Federal Office for Information Security (BSI) in February 2016. Schönbohm studied International Management in Dortmund, London and Taipei and has held leading positions in the field of IT security for more than 10 years. Before becoming CEO of BSS BuCET Shared Services AG (BSS AG) in 2008, Schönbohm held various positions at the European Aeronautic Defense and Space Company (EADS). Most recently, he was Vice President for Commercial and Defense Solutions at EADS.

www.bsi.bund.de

About

How does cybersecurity affect a company’s competitive edge?

Digitalization is a crucial factor for productivity and economic growth in Germany, and successful digitalization calls for information security. In an increasingly digitalized and networked business world, cyberattacks and threats pose extreme challenges to the economy. Without appropriate efforts to ensure the necessary degree of information security, companies and businesses are increasingly at risk.

What have been the biggest misconceptions you have encountered about cybersecurity in your work with companies so far?

CEOs used to think that cybersecurity should be handled by their companies’ IT departments. However, as they read in the news almost every day about the numerous cyberattacks we’ve had over the last few years and learned about the consequences a cyberattack can have on a business, they quickly realized that cybersecurity was not something the IT department alone should be taking care of. There will be no successful digitalization without cybersecurity.

How can cybersecurity be embedded in a company’s corporate culture?

Cybersecurity should be implemented on the C-level of an organization. Since cybersecurity is a decisive factor in the company’s success in a digitalized economy, it’s a management issue that needs to be addressed strategically. Top executives need to develop an understanding for the importance of cybersecurity in terms of corporate success. They need to be able to rate the potential monetary and
Successful digitalization calls for cybersecurity

AN INTERVIEW WITH ARNE SCHÖNBOHM, PRESIDENT OF THE GERMAN FEDERAL OFFICE FOR INFORMATION SECURITY (BSI), ABOUT CYBERSECURITY IN COMPANIES AND THE OPPORTUNITIES FOR TRANSATLANTIC COOPERATION TO PREVENT CYBERCRIME.

As important as it is to defend against concrete attacks from any part of cyberspace, we shouldn’t forget the fundamental issue of preventing potential attackers from attempting their attacks by implementing prevention measures. This requires both the further development of the legal framework, the development of security standards for IT structures, and the protection of critical infrastructures in coordination with the business community.

What can governments on both sides of the Atlantic do to fight cybercrime?

I can speak for Germany only. Safeguarding security in cyberspace and protecting critical information infrastructure are vital concerns of the 21st century and require a high level of government commitment. The German federal government has done more in terms of strategic development, legislation and practical measures for IT and cybersecurity than ever before. This includes, for example, creation of the IT Security Act in 2015, implementation of the EU’s NIS Directive, updating the ordinances on critical infrastructures in 2016 and 2017, development of a new Cybersecurity Strategy for Germany in 2016 and expansion of the BSI. The means the German government has implemented numerous measures to handle the risks posed by cyberspace. With the IT Security Act 2.0, Germany is currently expanding its regulatory framework to adequately counter new threats.

How does the BSI provide concrete support on cybersecurity issues?

Internationally, the BSI is a thought leader and competence center for all issues related to information security in multilateral and bilateral cooperations. A particular focus is on cooperation in the EU and NATO.