The Professionals' Perspective:
Cyber Security in the DACH Region

FROST & SULLIVAN

A Frost & Sullivan Market Study in Partnership with:

(ISC)²

(ISC)² FOUNDATION

A Frost & Sullivan White Paper

Authors:
Michael Ranke, Vice President, Customer Research
Jarad Carleton, Principal Consultant, Digital Transformation

contents

INTRODUCTION

For over a decade, (ISC)^2 has been at the vanguard of sponsoring global information security workforce studies that provide insight on cyber security challenges and how the workforce responds in a rapidly evolving business and security landscape. The cyber security challenge is global in nature, but the reaction to it is not always the same. Understanding the impact and different responses to similar challenges in different parts of the world broadens the understanding of the security profession.

The 2015 (ISC)^2 Global Workforce Study covers data collected from nearly 14,000 professionals around the world, including over 500 from the DACH region—Germany (D), Austria (A), and Switzerland (CH). This paper dives into the DACH responses to help professionals understand the security and business dynamics of the region. Information security professionals in DACH have provided insights about their work environment that highlight strengths and shortfalls in the regional response to the security challenge, and illuminate the drivers for priorities in budget spend and recruitment needs. Professionals in DACH have the opportunity to compare their organization to the regional average to help with business planning over the next two years, and facilitate data-driven conversations with top-level executives that need to better understand the cyber security challenge.

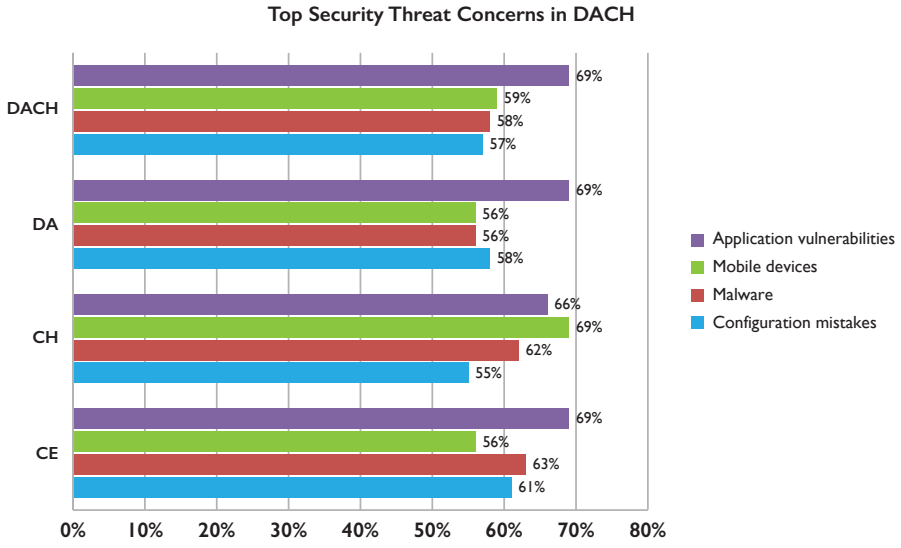
To provide the appropriate context for business planning and these conversations, the data is almost always presented for the DACH region as a whole, as well as for DA, CH, and Core Europe (CE).[1]

Although there are a few differences between DA and CH, the biggest difference of all is a well-known fact: information security professionals in CH are paid more. In fact, by splitting the region in two, one can see that DA and CE salaries are aligned, while CH is 36.8% more expensive.

1 Core of Europe is defined as continental Western Europe, Scandinavia, and the UK.

The Landscape: Top Concerns and Threats

In examining the most common security threats in DACH, information security professionals highlight an interesting difference between top security concerns and the most common security threats detected. Further, information security professionals in CE and DACH are concerned about similar threats, although there are some differences regarding which are more important.



Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

Application vulnerabilities are a top concern in DACH and CE, just as they are around the world. It's well known that software developers are under pressure to release new products according to aggressive schedules set by executives. In the rush to get an application to market, poor development practices are followed, while limited or often no security testing and scanning is performed. Unfortunately, the rush to release a new product before a competitor continues to trump the need for more secure applications. Hackers understand this dynamic, as do information security professionals, which is why application vulnerabilities are a top concern.

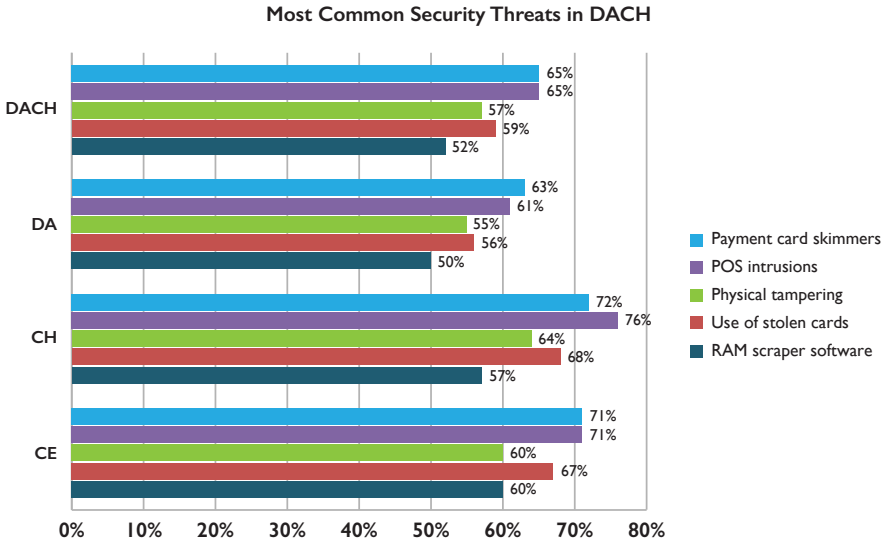
Mobile devices are one of the more interesting areas of difference in the DACH region. Globally, there has been a notable downward trend in concern over mobile devices that DA and CE data appear to confirm. In CH, however, there is a markedly different perspective. Security concerns about mobile devices are 13% higher than DA, making it the top concern for that part of the region. It's very likely that CH is more sensitive to the security threat mobile devices pose because it is a world leader in offshore financial services and has substantial intellectual property tied to its MEM[2] and chemical/pharmaceutical industries.

Malware continues to be a concern for information security workers as employees continue to be easily tricked with social engineering techniques to click on files and links from unknown senders. Overall, DA information security professionals are slightly less concerned about malware (56%) than their counterparts in CH and CE (62% and 63%, respectively). Since it is not plausible that DA has a lower incidence of malware, a possible explanation could be different approaches to data breach prevention or a different ratio of employees with access to the Internet at work.

2 Die Maschinen-, Elektro- und Metallindustrie

Configuration mistakes, a new option in the survey this year, rounds out the list of top security concerns for DACH and CE. The high level of concern regarding configuration mistakes illustrates the known potential for a serious security breach as a result of human error. Unfortunately, the concern about configuration mistakes will likely remain high due to employment and training gaps—topics that are addressed later in this paper.

Looking at the threats there appears to be a disconnect between what is being detected and what is identified as a top concern. A practical explanation could be that the financial services, retail, and service sectors have a lot of resources devoted to combat payment card fraud. This is particularly true in CH, which has a large financial services sector. While top threat concerns highlight areas where information security professionals need more resources to effectively deal with evolving security threats, it is worth noting that companies' preparedness could lag current requirements.



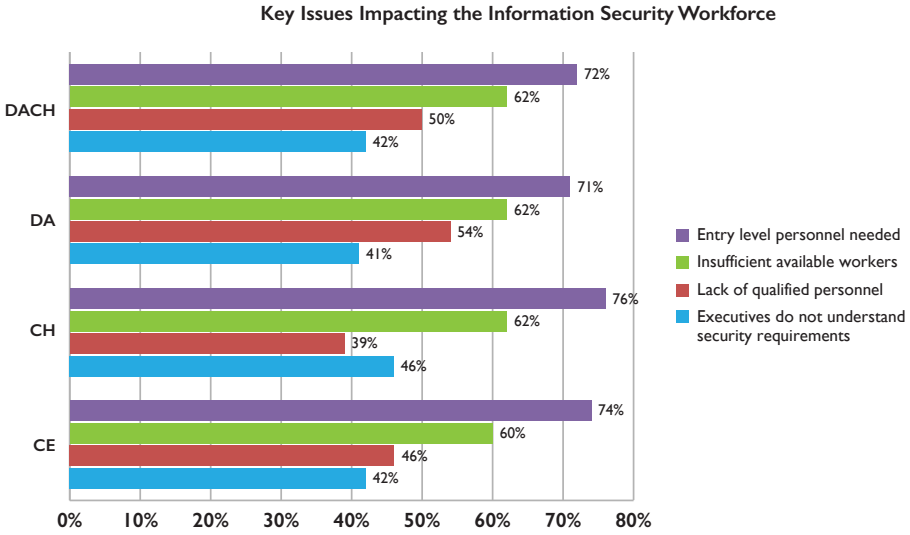
Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

Security Complexity and Architecture Sprawl

The security ecosystem in which information security professionals work shows no signs of becoming less complex. The leading factor contributing to security complexity is architecture sprawl, a problem defined by an increasing number of security vendors and consoles, and only a trivial improvement in security posture. Of DACH information security professionals, 57% identify sprawl as an operational concern. This isn't surprising since sprawl is a significant management burden for workers that have to train with security products from multiple vendors and filter through more noise in security reports to find real threats. That's why 54% of DACH professionals believe that sprawl has hindered security efficacy and created training challenges for their organizations.

Its roots in DACH stem from decentralized purchasing of security technology (21%), mergers and acquisitions (27%), and threats that evolve faster than security products (34%). Ironically, a key reason for sprawl is the evolving threat landscape itself as organizations buy additional security products in response to new threats. The value of this tactic is, however, unclear because today, three out of every five data breaches in DACH are attributed to a previously unknown vulnerability. The strategy of throwing more security products at a problem clearly isn't as effective as some hoped it would be.

Employment Gaps



Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

The high demand for entry-level information security workers across the DACH region and the lack of available workers is a familiar theme across CE and the world. On average, information security professionals across DACH cite the need to increase staff by 11%. The most needed professionals in DACH are:

- Security analysts;
- Forensic analysts; and
- Security architects.

The need for these professionals puts a spotlight on the challenges that the respondents identified; for example, the need for critical analysis on malware inside an organization, and insights on the 60% of DACH data breaches attributed to unknown vulnerabilities. The need for security architects makes sense in light of the concern expressed with technology sprawl and evolving influences on systems such as mobility.

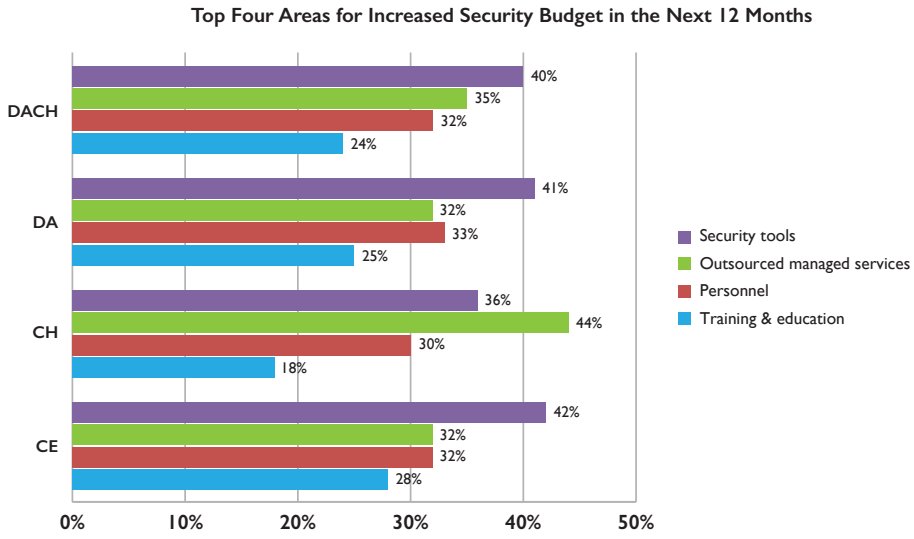
Though the cause of the personnel shortage in DACH can be traced to several factors in the market, one thing is clear: higher salaries make it easier to find the most needed workers. That is a key reason that CH organizations have less difficulty locating and hiring qualified personnel.

THE RESPONSE

Security Budgets

Security spending in DACH averages €3.58 million per organization annually,[3] almost half a million Euros more per year than CE. In response to personnel gaps, security complexity exacerbated by architecture sprawl, and the inability to stop data breaches, organizations are turning to advanced analytics solutions to understand where to focus their security efforts.

3 Based on 27 August 2015 exchange rate from USD to Euro = 0.884..

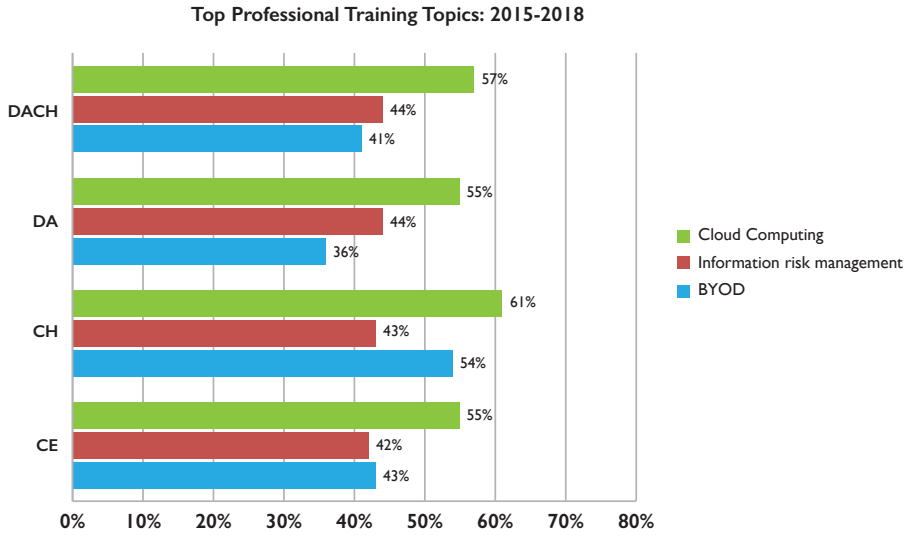


Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

In 2014, 26% of DACH companies had implemented an advanced analytics solution and 15% were in the process of implementing one. Analytics use in DACH is slightly higher than CE where installed advanced analytics versus solutions being implemented were 22% and 14%, respectively.

In addition, strategically outsourcing some security functions surfaces as another way to make up for personnel gaps, a coping technique that appears high on the agenda for CH organizations in 2015. Budget spending for professional training and education is also on the rise, suggesting an appreciation for the level of change that is taking place in the field of practice.

Professional Training, Certifications, Experience, and Communication Skills

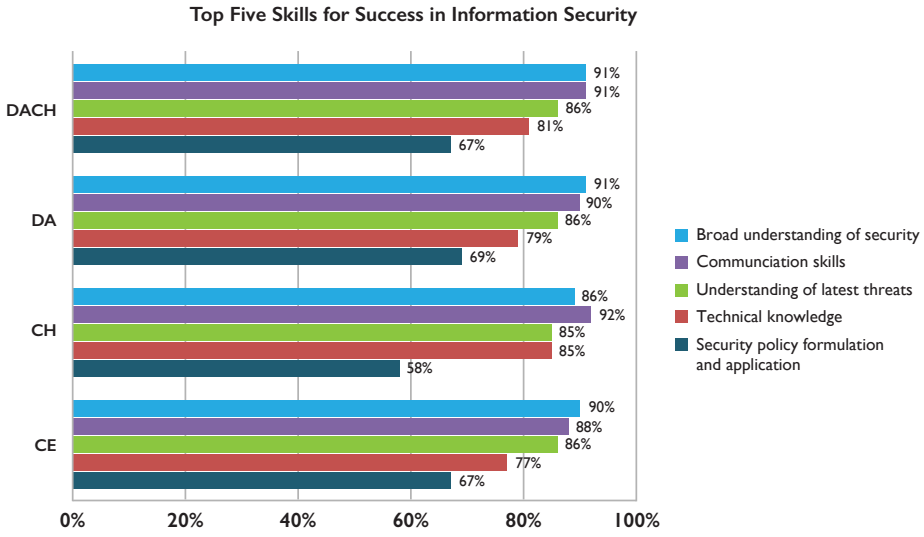


Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

The leading professional training topic in DACH is cloud computing, a sensible choice since 43% of the region uses cloud services today and another 10% plan to use them within the next two years. Not surprisingly, information risk management training is also a priority as organizations try to improve the process of assessing the value of information resources in the company, identifying vulnerabilities, and choosing appropriate countermeasures. Of course, BYOD training is a high priority for CH organizations because mobile devices are the top security threat concern for that part of the region.

Professional certifications are a strong indicator of the desire to communicate experience and a proactive effort to achieve the skills for success in information security; 59% of DACH respondents said professional certifications are "important" or "very important."

Information security professionals also identified the skills they believed were essential for success. It is interesting to note that technical knowledge ranks lower than the need for a broad understanding of security concepts and communications skills. This sits in sharp contrast to the driving trends behind technology sprawl.

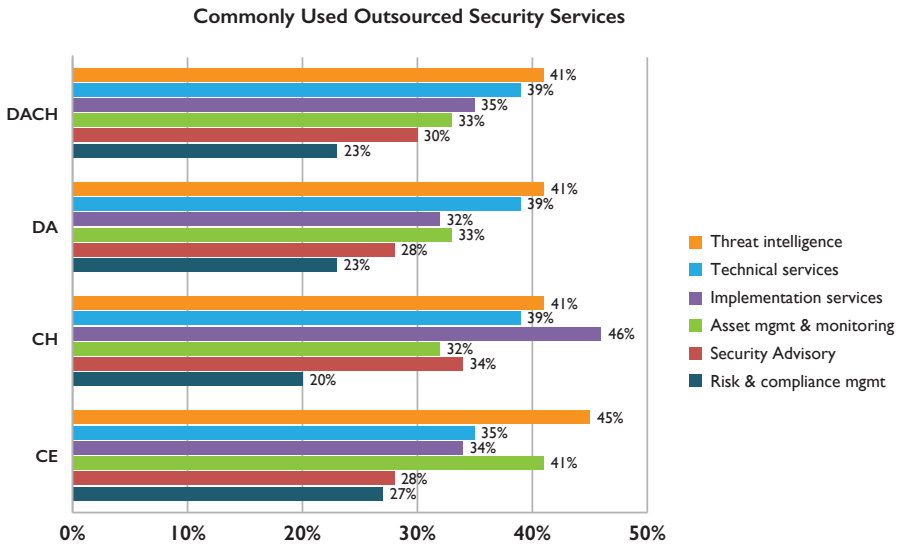


Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

Outsourcing

The constant evolution of security threats and the persistent deficiency of qualified and available workers are driving DACH companies to outsource some security services. Since DACH organizations are using outsourcers to address personnel shortages, it makes sense that one of the top criteria for choosing a security services provider is the number and quality of the security staff.

Two of the top outsourced services in DACH are threat intelligence and implementation services. They are complimentary because they empower organizations to more efficiently tackle enduring security challenges identified by the DACH workforce. The use of threat intelligence, which is customized for an organization, provides a broader view of the security landscape for the DACH workforce and provides actionable recommendations to correct weaknesses. When threat intelligence is combined with implementation services, DACH organizations with personnel shortages still have the ability to quickly remediate threats as they evolve, which is why both services are important in the region.



Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH and Core Europe, N = 2,801

THE LAST WORD

Many of the challenges for the DACH information security workforce stem from persistent personnel shortages. The lack of available personnel to fill the gap will hinder the ability of the workforce to gain more clarity and proactively address the top threat concerns of the region. There is a clear need to improve data breach prevention where 60% of all breaches are linked to previously unknown vulnerabilities. Professionals have the opportunity to push organizations to spend security budget in strategically different ways that address the concerns they have illuminated here. Steps are being taken to enhance professional training, and invest in the advanced analytics solutions and threat intelligence services that should enable more informed decisions around the tactics, solutions and the purchase of security tools. This paper was developed for DACH professionals to offer reliable reference data for business planning and career growth. With 2016 on the horizon, it is hoped that the insights from this paper can inform productive conversations that influence information security budget and planning.

ABOUT (ISC)²® AND THE (ISC)² FOUNDATION

(ISC)² is the largest not-for-profit membership body of certified cyber, information, software and infrastructure security professionals worldwide, with nearly 110,000 members. www.isc2.org

The (ISC)² Foundation is a non-profit charitable trust that aims to empower students, teachers, and the general public to secure their online life by supporting cybersecurity education and awareness in the community through its programs and the efforts of its members. Through the (ISC)² Foundation, (ISC)²'s global membership of nearly 110,000 certified cyber, information, software and infrastructure security professionals seek to ensure that children everywhere have a positive, productive, and safe experience online, to spur the development of the next generation of cybersecurity professionals, and to illuminate major issues facing the industry now and in the future. For more information, please visit www.isc2cares.org.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041