Technical Report

SIDATE

IT Security Status of German Energy Providers

The following people contributed to this report:

Julian Dax, University of Siegen
Ana Ivan, Goethe University Frankfurt
Benedikt Ley, University of Siegen
Sebastian Pape, Goethe University Frankfurt
Volkmar Pipek, University of Siegen
Kai Rannenberg, Goethe University Frankfurt
Christopher Schmitz, Goethe University Frankfurt
André Sekulla, University of Siegen

Published in 2017, University of Siegen, Siegen

Secure information networks of small- and medium-sized energy providers (SIDATE)

The focus of the SIDATE research project is the technical support of small- and medium-size energy providers for the self-assessment and improvement of their IT security. Different concepts and tools are developed and evaluated by the University of Siegen, Goethe University Frankfurt, regio iT Gesellschaft für Informationstechnologie mbh, and Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung (ASEW).
More information is available on the project's website http://sidate.org/ .

Funding

This research project was funded by the Federal Ministry of Education and Research (BMBF) as part of the funding focus "IT Security for Critical Infrastructure".

Image credit

Image on title: ©TebNad / Fotolia

Table of Contents

Introduction

As part of the research project "Secure information networks of small- and medium-sized energy providers" (SIDATE), a survey about the IT security status of German energy providers was conducted. The project itself is focused on the IT security of small- and medium-sized energy providers.

In August 2016, 881 companies listed by the Federal Network Agency were approached. Between, September 1st 2016 and October 15th 2016, 61 (6.9%) of the companies replied. The questionnaire focuses on the implementation of the regulatory requirements and on the implementation of an information security management system (ISMS). Additionally, questions about the energy control system, the network structure, processes, organisational structures, and the IT department were asked. Questions were asked in German, so all questions and answers are translated for this report.

Subsequently, the result of the survey is presented. Some questions were only answered by very few participants, and therefore, the related results are not presented.

The survey is organised as follows:

A) General Company Information
B) Organisational Aspects
C) Information Security Management System (ISMS)
D) Office IT
E) Energy Control System: Network Structure
F) Energy Control System: Processes and Organisation

There are two different types of bar charts. The first only contains blue bars. These charts pertain to all energy providers that replied to the specific question. In contrast, the second type of bar charts presents a categorical differentiation between energy providers. The differentiation lies in the size of the company, which is represented by the number of corresponding meter points.

In some cases, spider-web diagrams were used. A categorisation of the responding companies was once again not included in these cases.

Part A: General Company Information

In the first part of the survey, general questions were asked in order to present an overview of the participating energy providers. Based on the replies, the energy providers were classified in four overarching categories, in order to achieve a better analysis of the following survey items.

The categorization of the participants uses the number of meter points of the providers as a criterion. The distribution by size is depicted in Figure 1. For the remaining analyses, the providers are separated into the following categories: small (between 0 and 15,000 meter points), medium (between 15,001 and 30,000 meter points), large (between 30,001 and 100,000 meter points), and very large (more than 100,001 meter points).

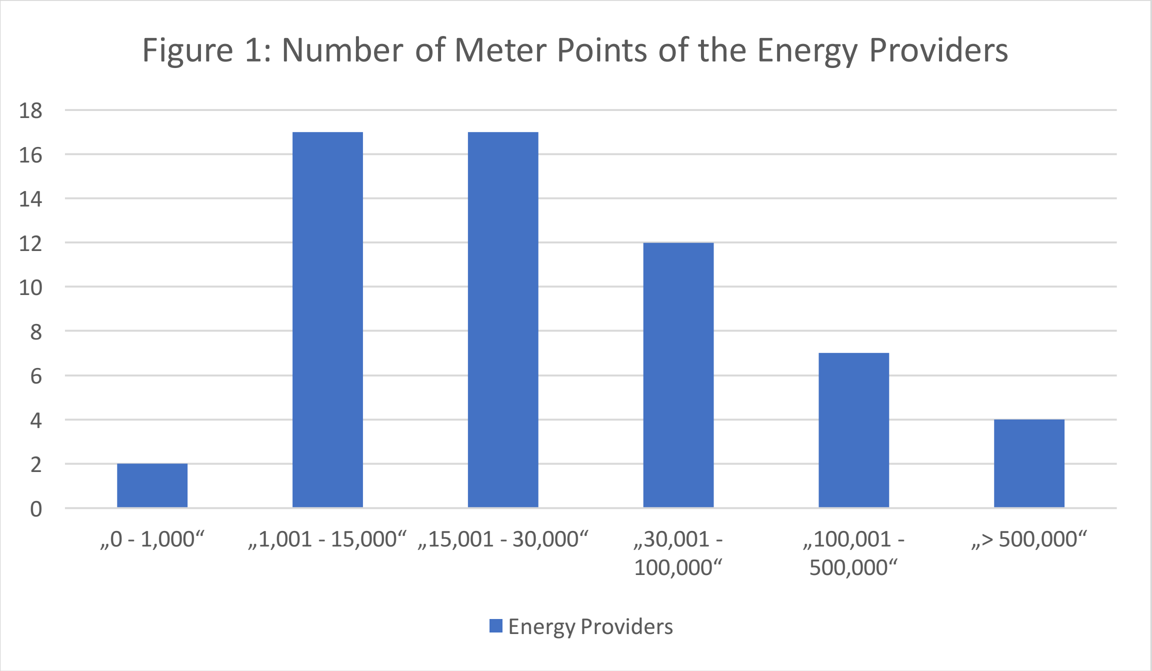


Figure 1: How many meter points are in your network?

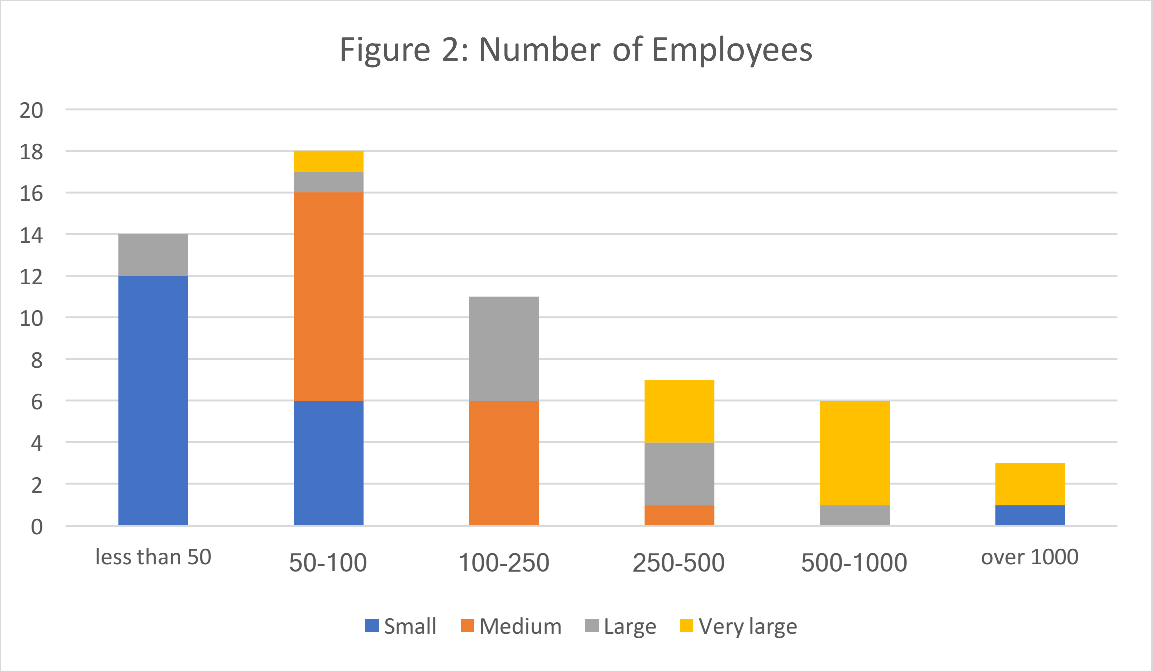


Figure 2: How many employees are in your company?

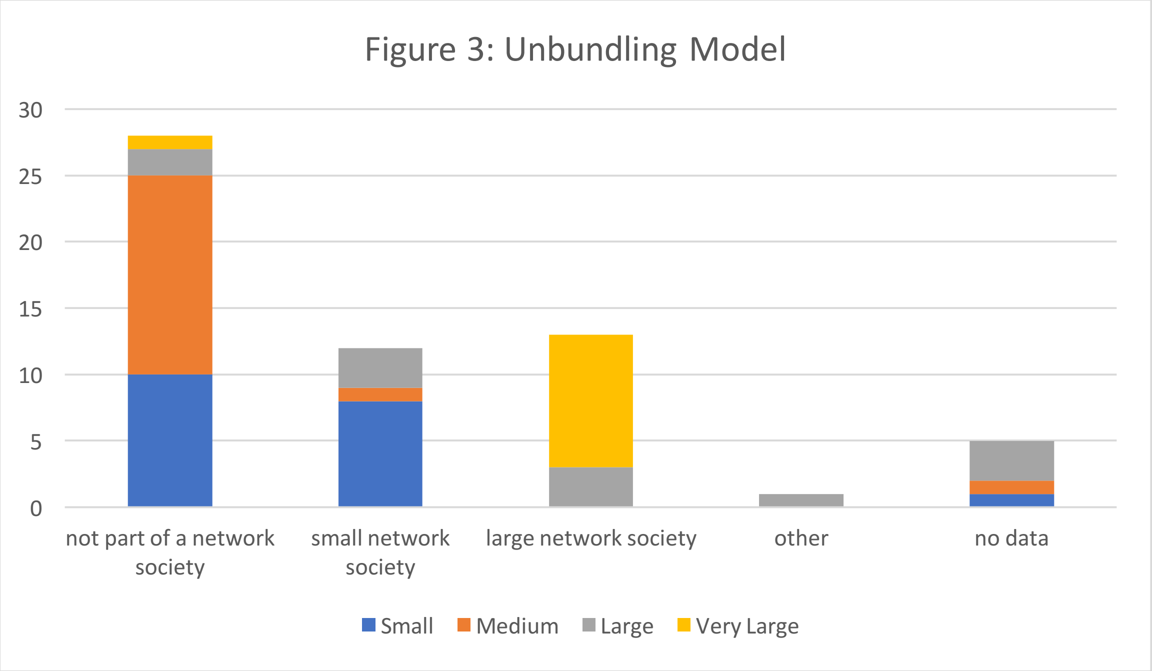


Figure 3: Which unbundling model is implemented in your company?

Part B: Organisational Aspects

In this section of the survey, questions about organisational matters were posed. Subsequently, questions about the particularities of the responding employees were included. Examples thereof include items about their job position within the company, or the department they are part of. Furthermore, concrete questions about the IT security were asked.

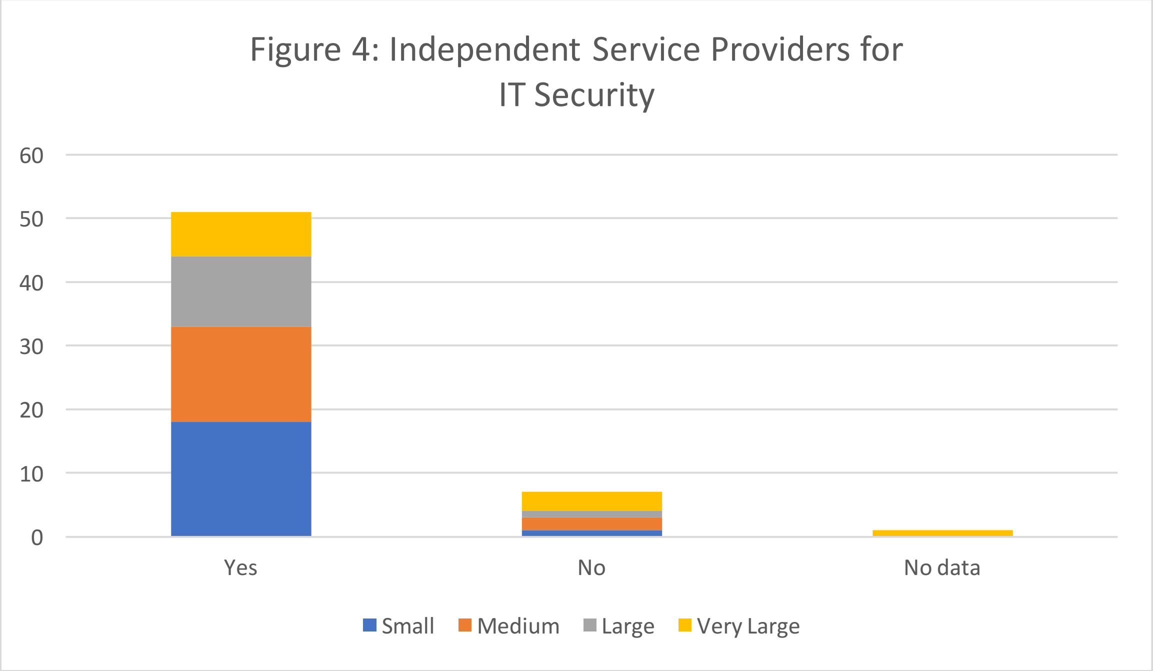


Figure 4: Are independent service providers in the field of IT security in your company?

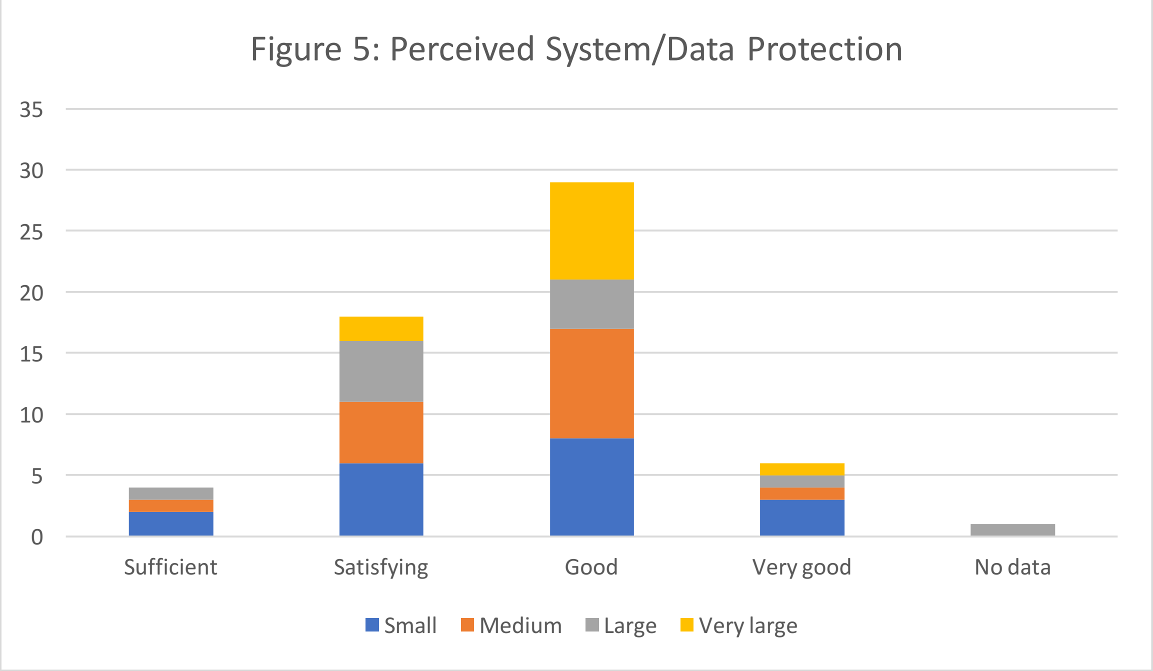


Figure 5: In your view, how well protected are the systems and data in your company?

Part C: Information Security Management System (ISMS)

In order to provide an overview of the implementation status of information security management systems, the survey was designed with specific related questions.

Figure 6: Overview of the ISMS Implementation Status

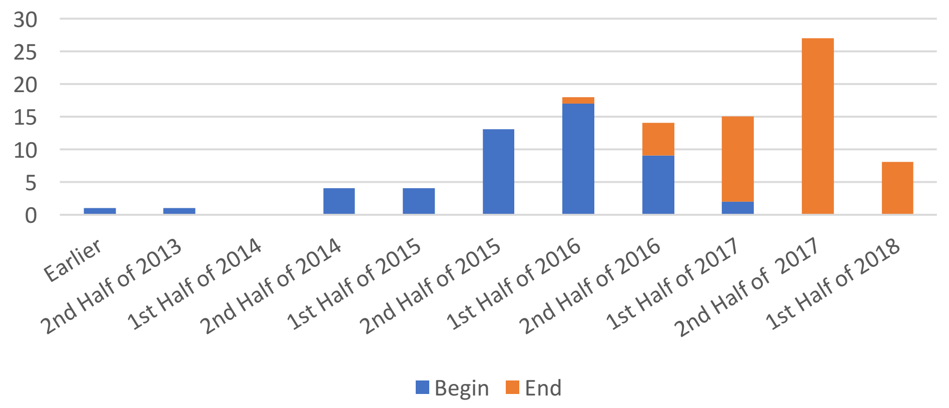
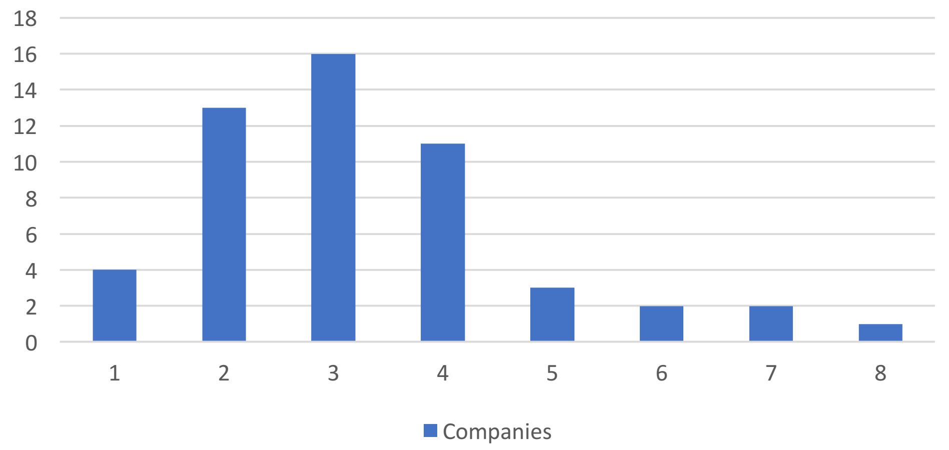


Figure 7: Duration in Half-Years



Figures 6 and 7 present the results of the following survey items:

- The implementation of ISMS …
- When are the ISMS implementation tasks supposed to start?
- When did the ISMS implementation begin?
- When is the ISMS implementation supposed to be finished?
- When was the ISMS implementation finished?

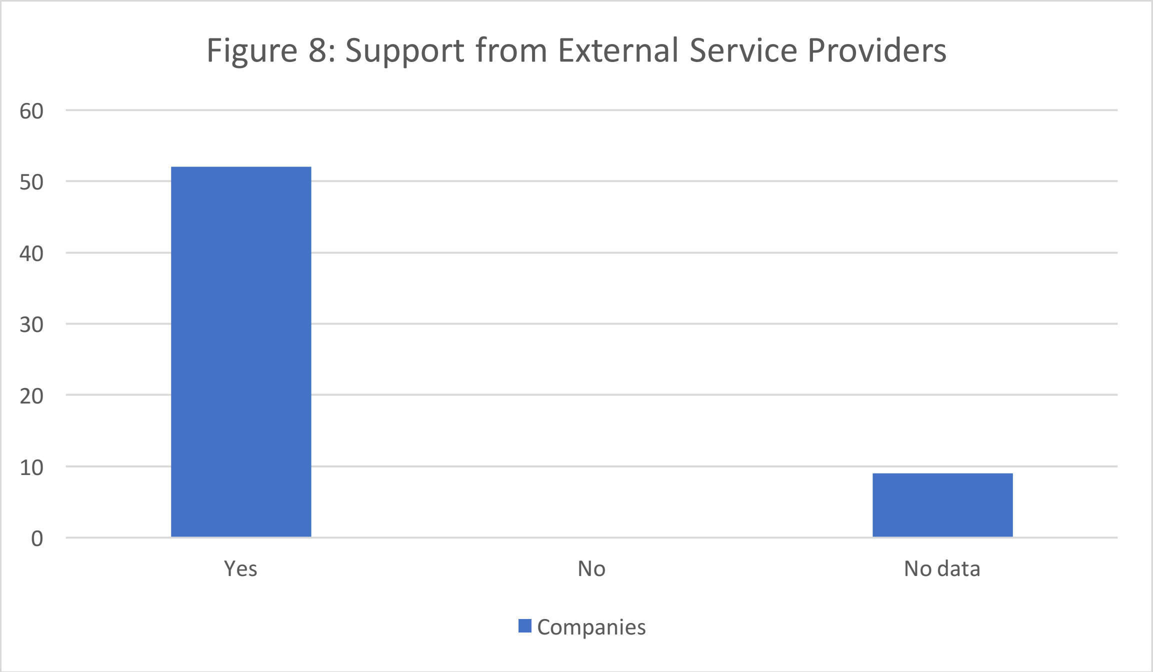


Figure 8: Were/Are external service providers (e.g. management consultants) subcontracted for the ISMS implementation?

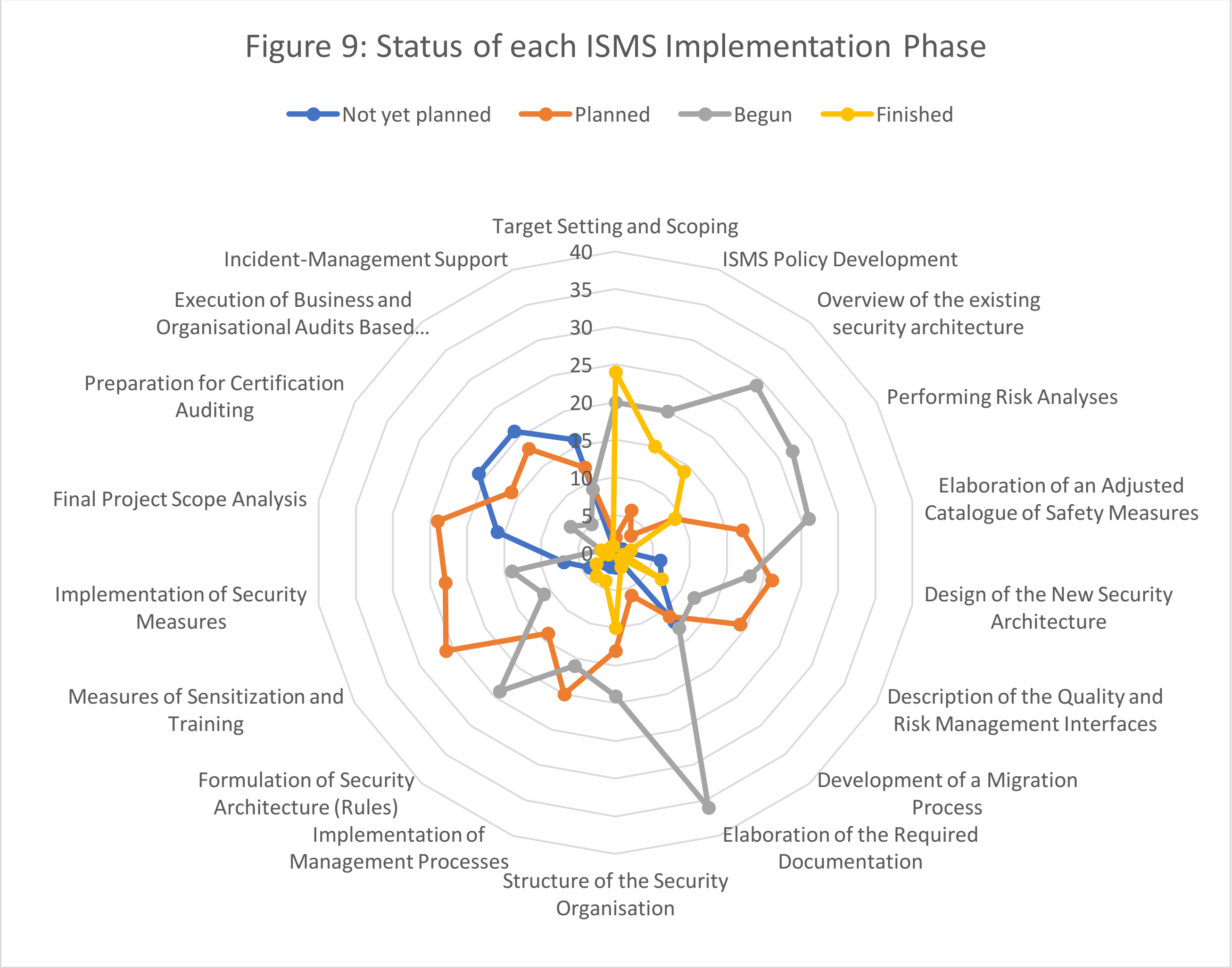


Figure 9: What is the current status of each ISMS implementation phase?

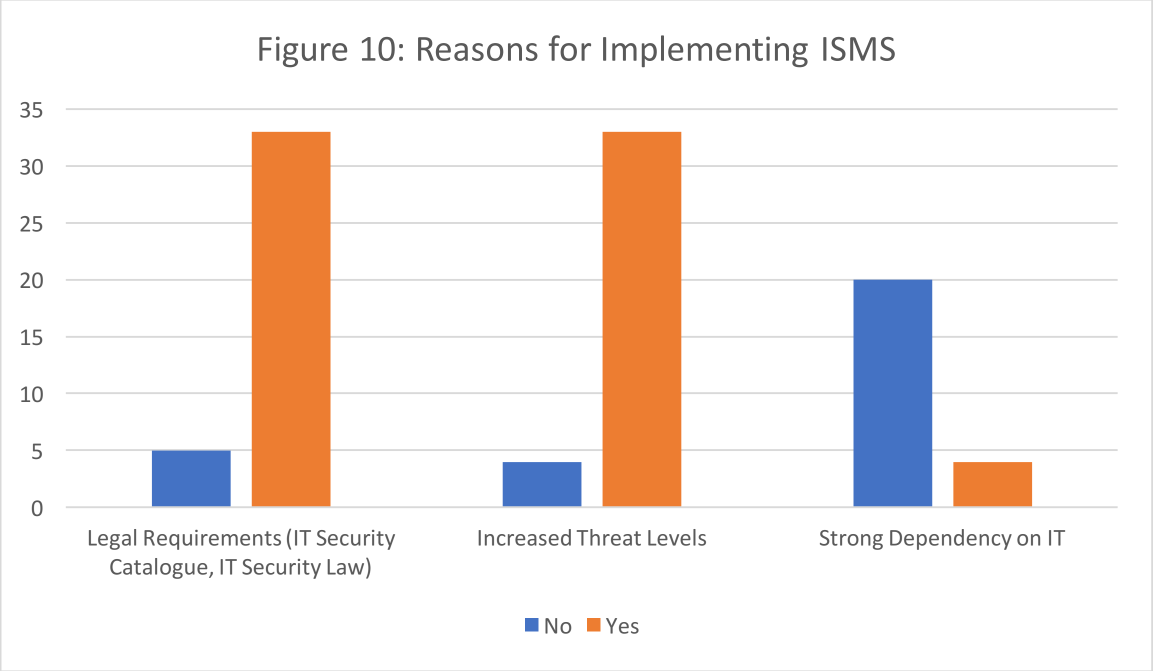


Figure 10: What were your reasons for implementing ISMS? (Multiple selection possible)

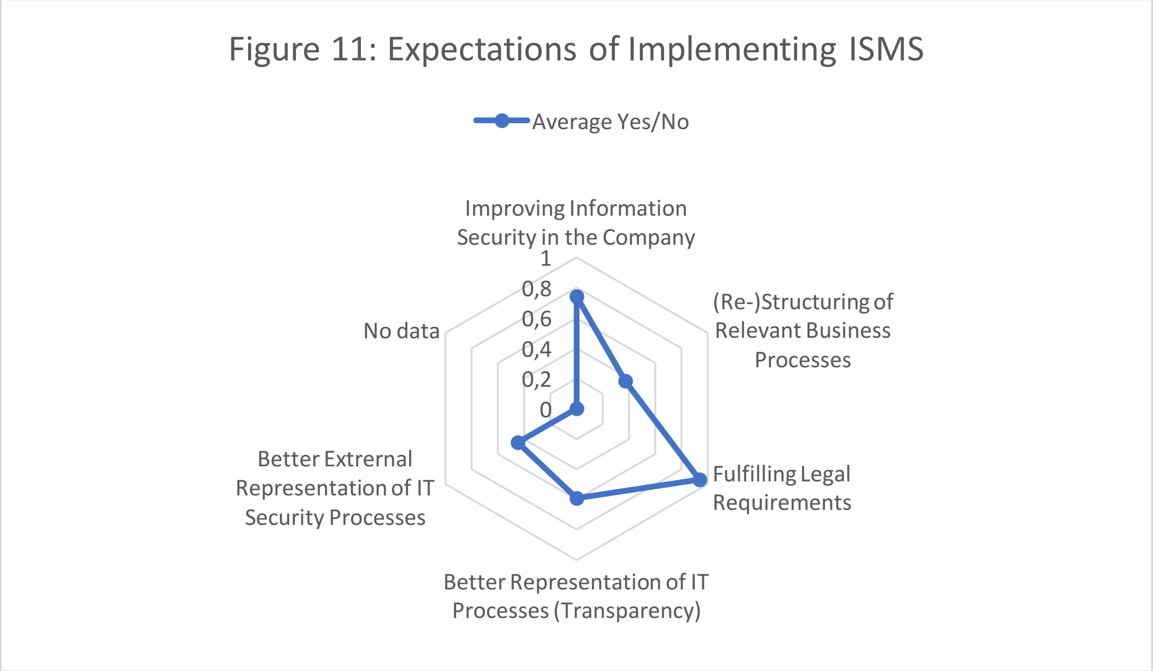


Figure 11: What are your hopes and expectations with regard to the ISMS implementation? (Multiple selection possible)

Part D: IT Department

This section of the survey deals with the aspects of the IT security of the office IT. In order to be able to guarantee higher security levels, there must be corresponding IT security guidelines, which must be evaluated regularly. The evaluation is important, given the continuous technical advances.

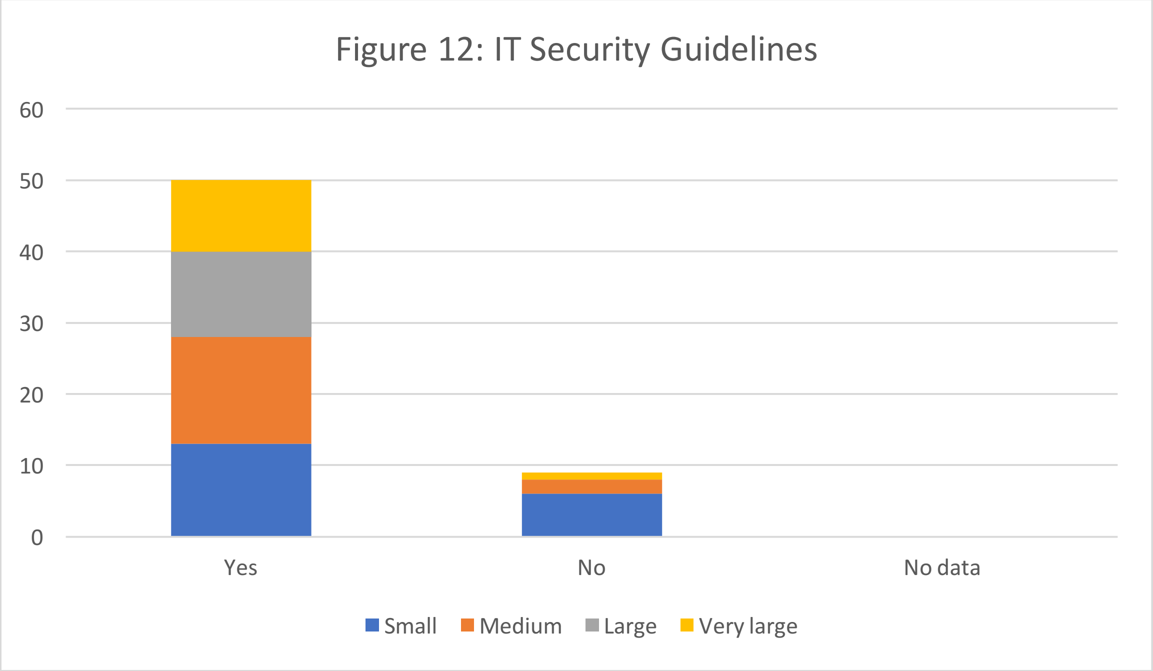


Figure 12: Are there IT security guidelines for the office IT in your company?

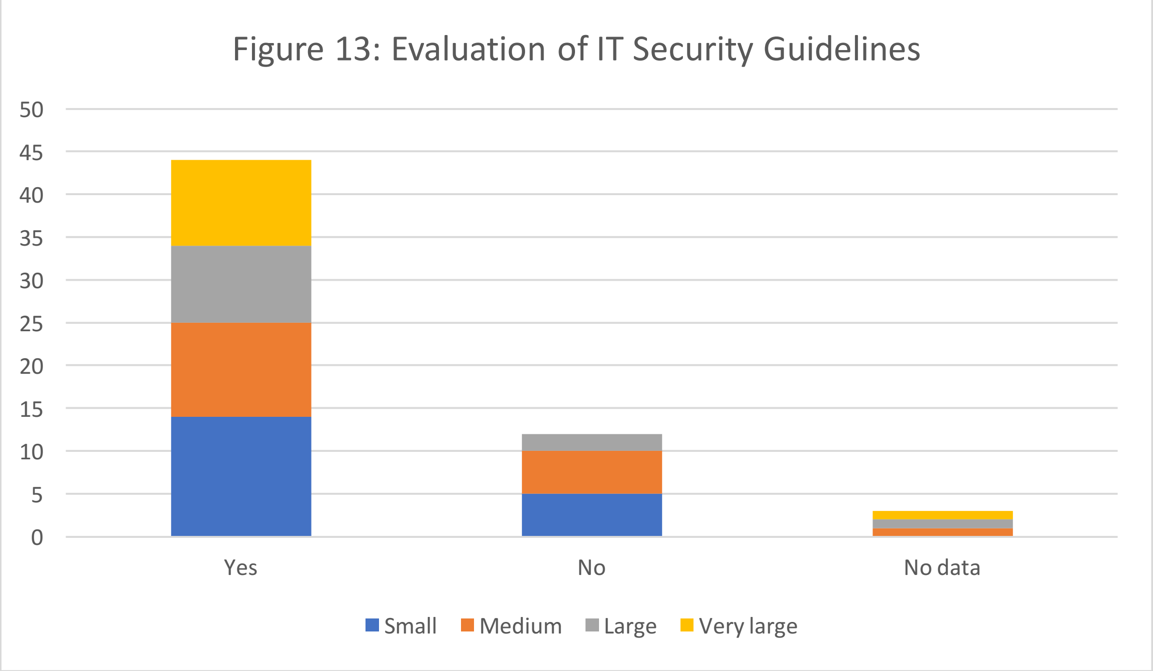


Figure 13: Are the IT security guidelines updated and, if necessary, adjusted regularly?

Part E: Energy Control System: Network Structure

The energy control system is the core system of the energy providers. Particular questions about the network structure were included in the survey in order to gather more information on the general structure of the energy control system. Two main tasks of the energy control system are the energy network supervision and control, and the execution of switching operations.

Another important aspect of the network structure is the separation between the energy control system and other networks (e.g. office IT; Internet; 3rd parties). If there is no separation threats and potential attack points may exist and need to be mitigated.

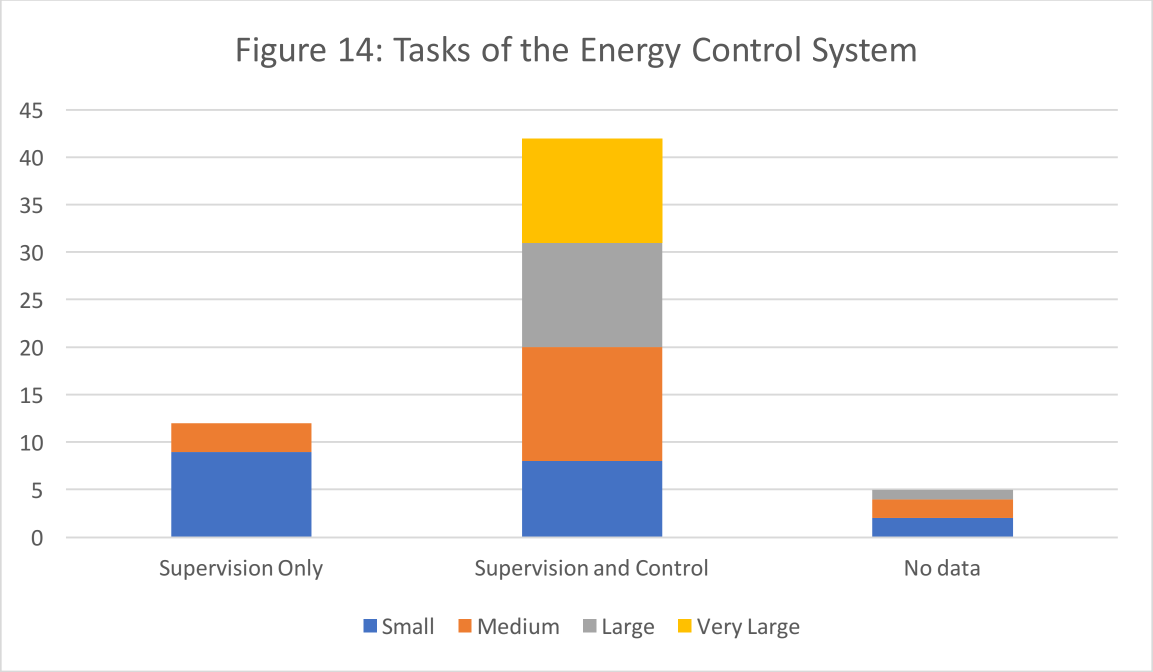


Figure 14: Does your energy control system undertake only energy network supervision, or can it also execute switching operations?

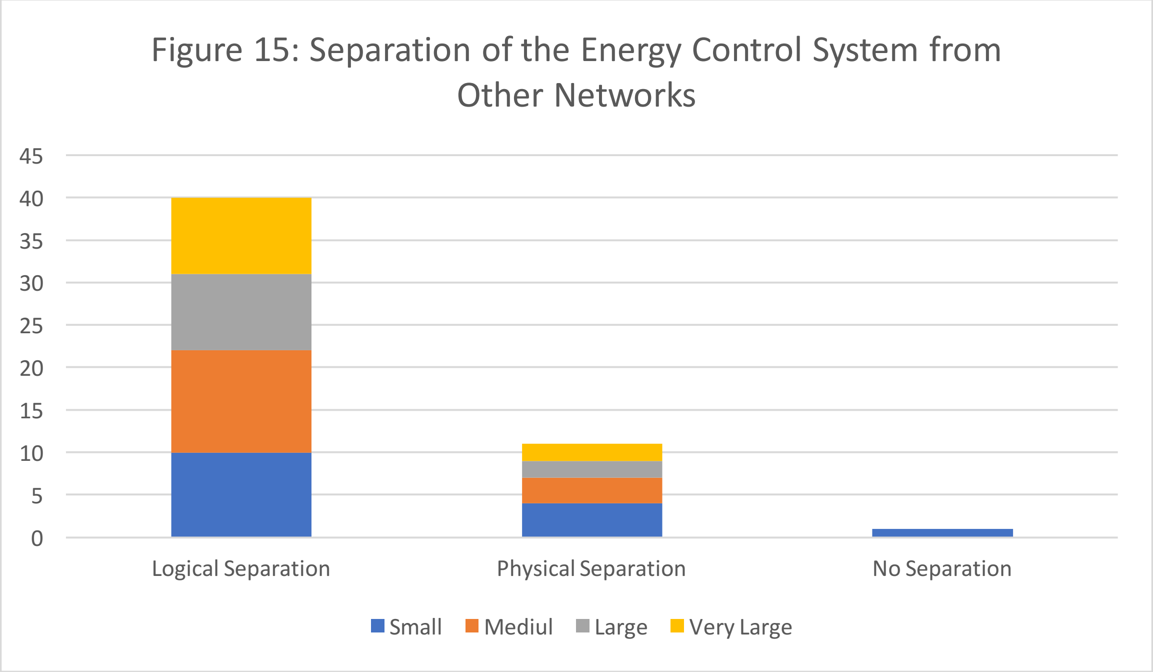


Figure 15: How is the IT network of your energy control system separated from other networks (e.g. IT department, Internet, maintenance companies)?

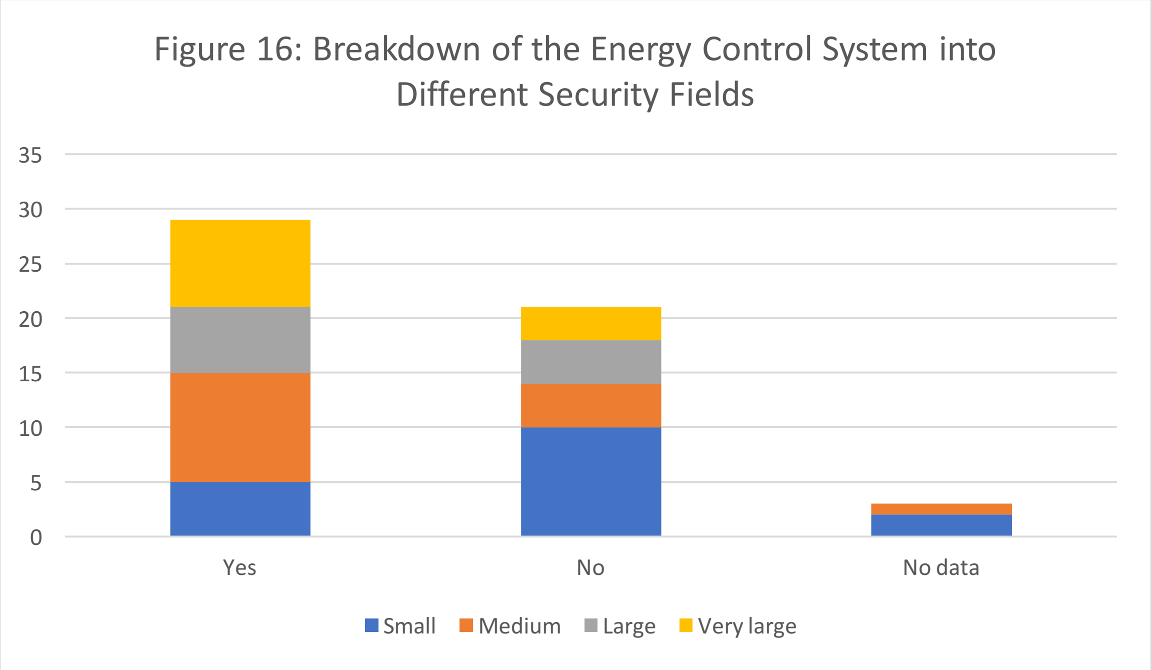


Figure 16: Is the network of your energy control system divided in different security domains (e.g. through different VLANs)?

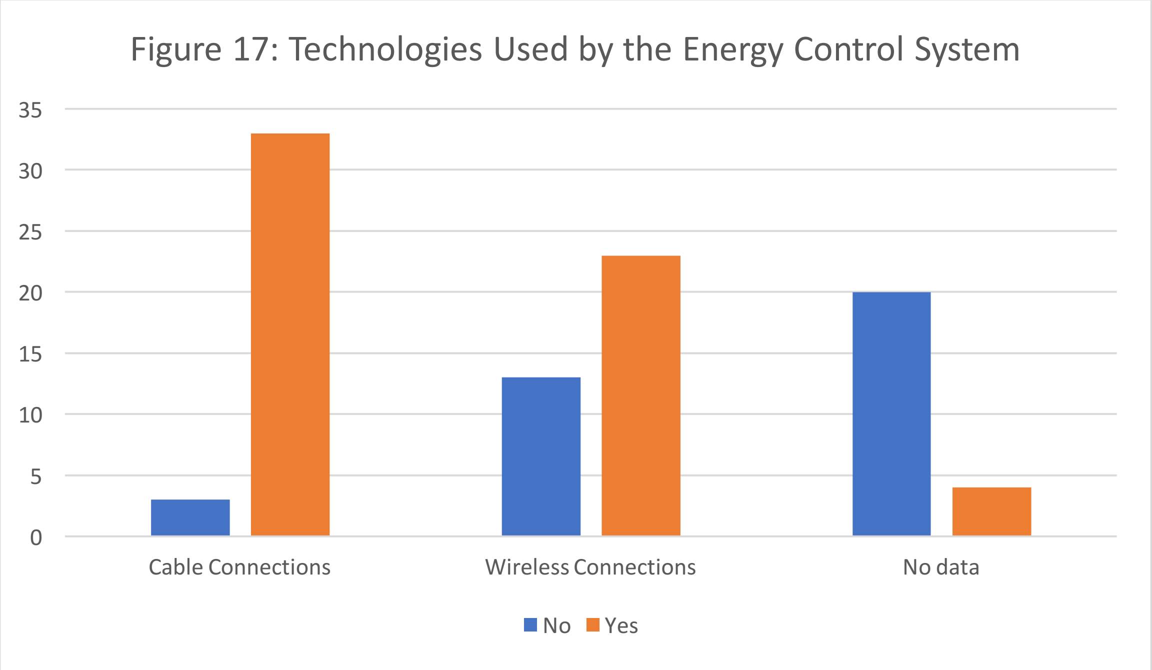


Figure 17: Which network technologies do you use in your energy control system network? (Multiple selection possible)

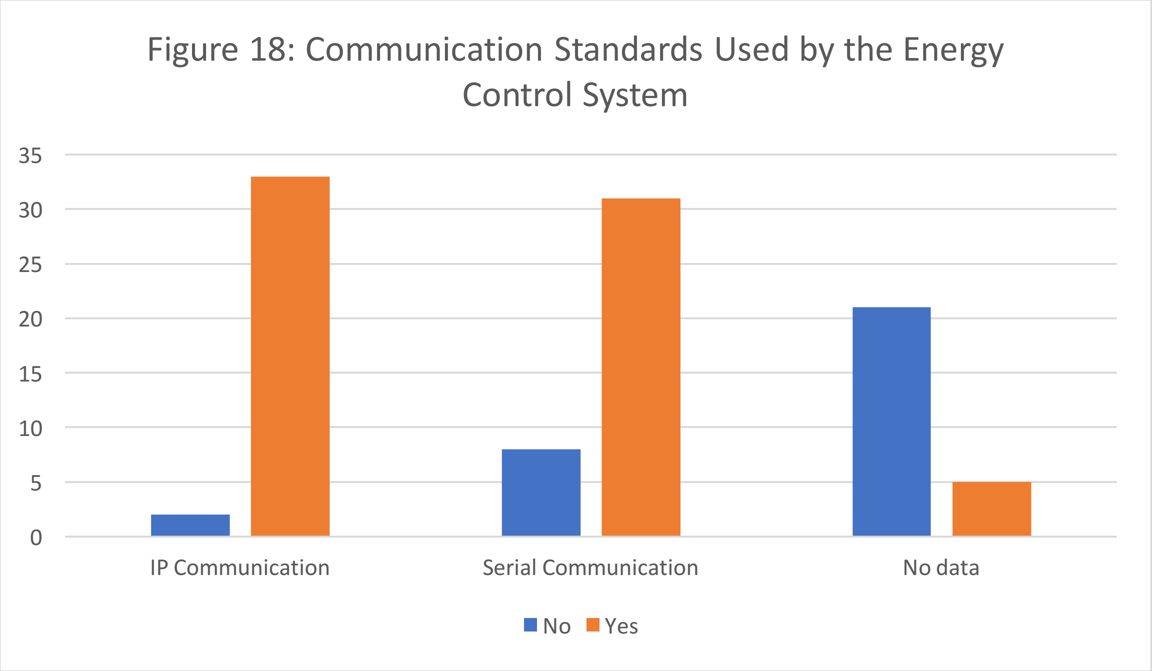


Figure 18: Which communication standards are used in the network of your energy control system?

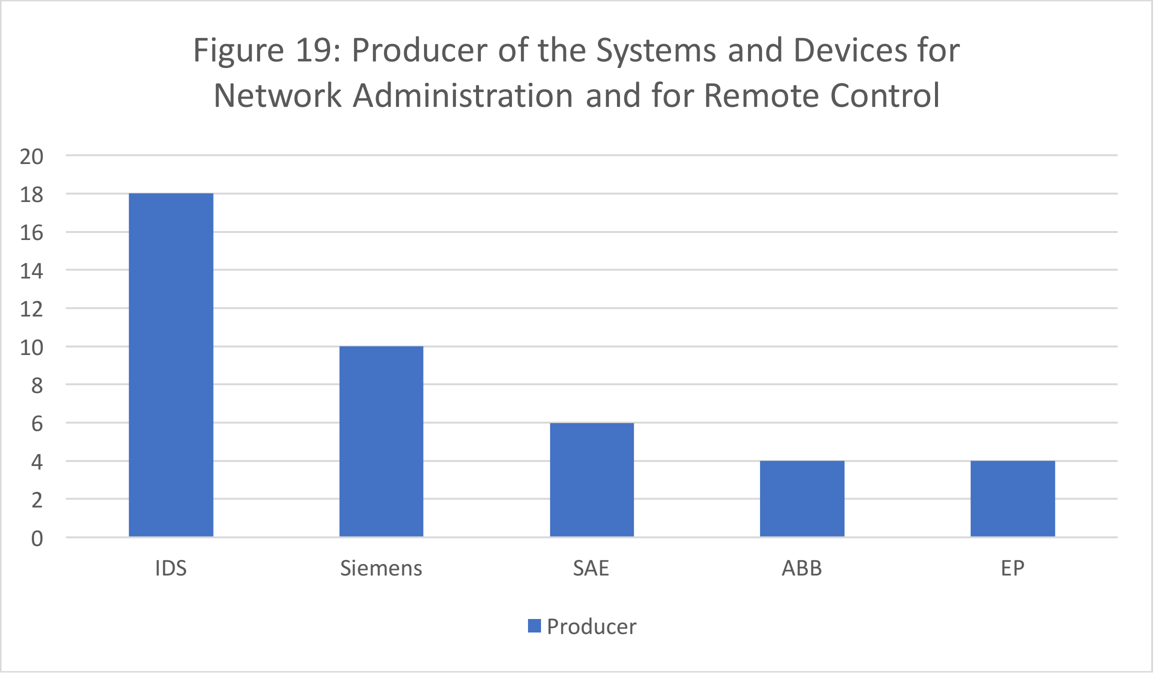


Figure 19: From which producers do you acquire the network administration systems and devices? (only producers with more than four nominations are depicted in the figure)

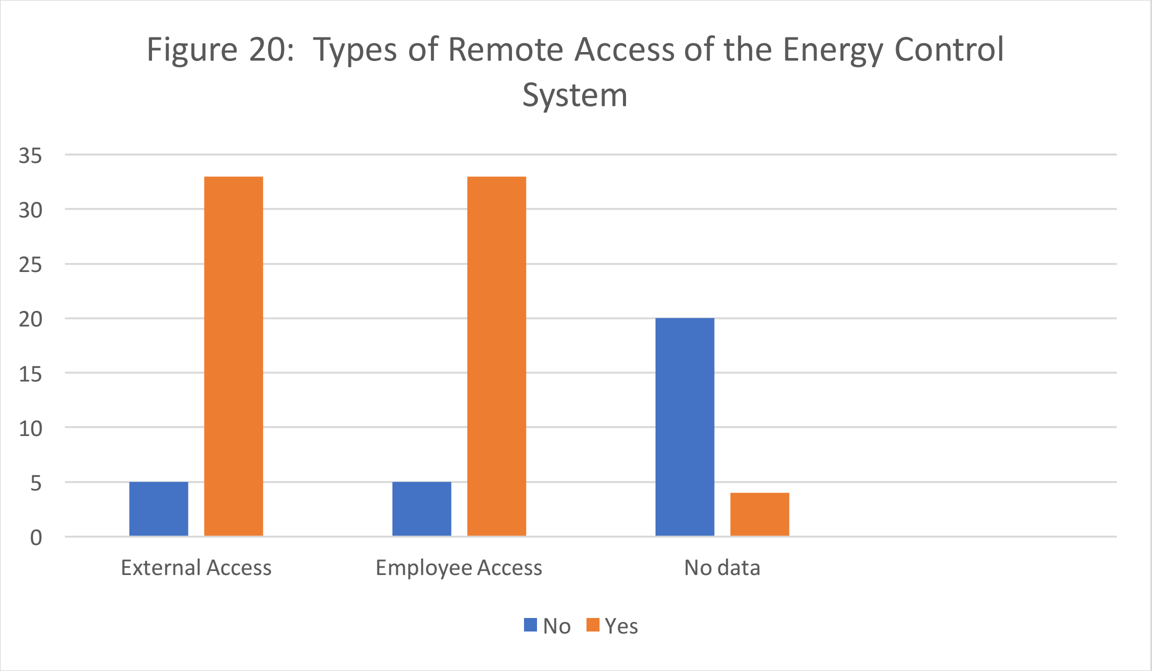


Figure 20: Which types of remote access were established for your energy control system? (multiple selection possible)

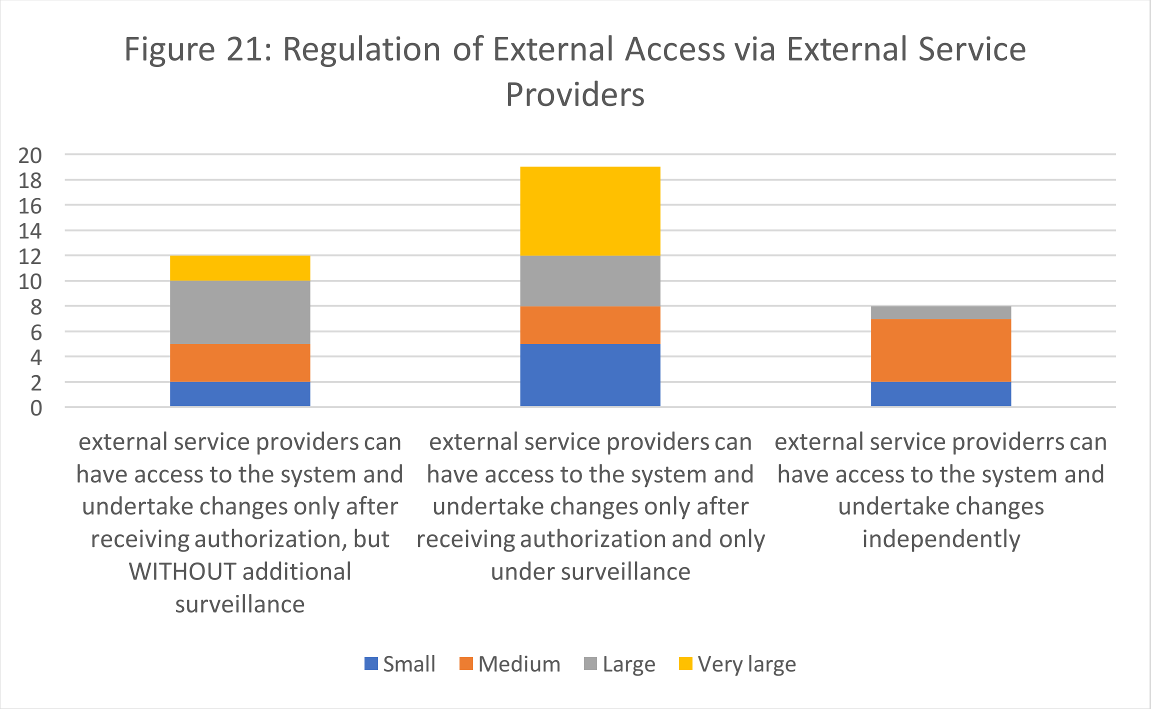


Figure 21: How are remote access procedures via external service providers regulated?

Part F: Energy Control System: Processes and Organisation

Apart from the technical data of the energy control system, the underlying organisational structures and processes are also important. IT security must be continuously supervised and improved, since the means and technologies of potential attackers evolve constantly. At the same time, vulnerabilities must be dealt with, and there must be regular supervision and information dissemination within the company, such that hacker attacks can be prevented.

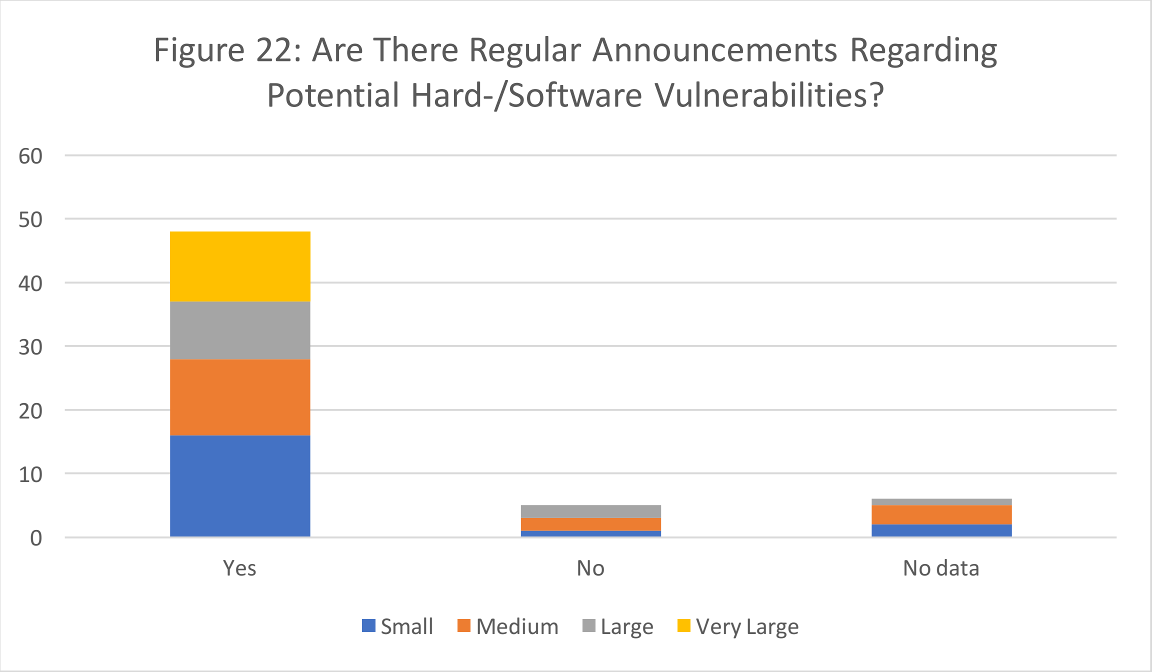


Figure 22: Are you/the responsible employees regularly informed about potential hard-/software vulnerabilities?

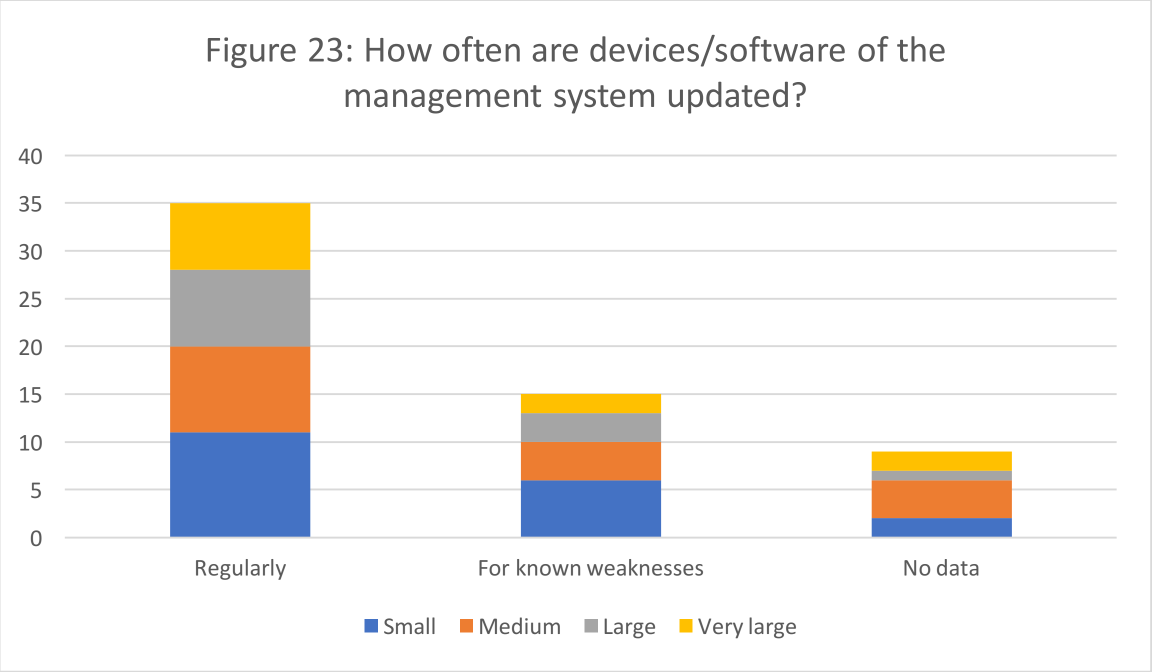


Figure 23: How often are the devices and software within your energy control system updated/renewed?

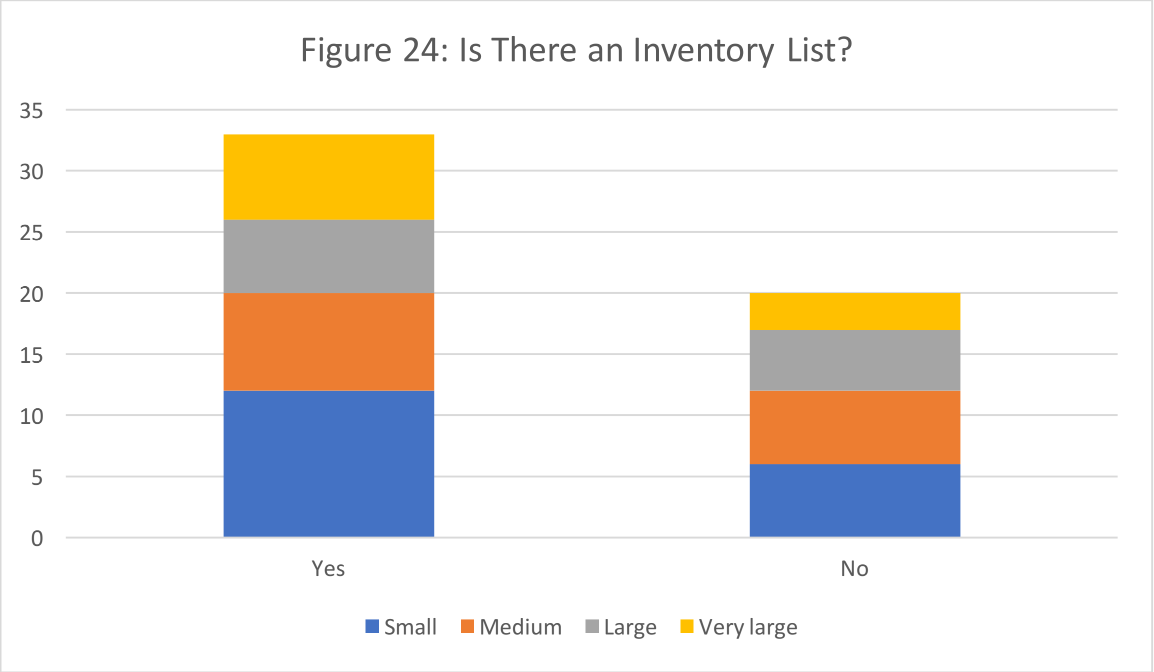


Figure 24: Is there an inventory list in which all the software items are documented (e.g. with version numbers, corresponding accounts and IP addresses)?

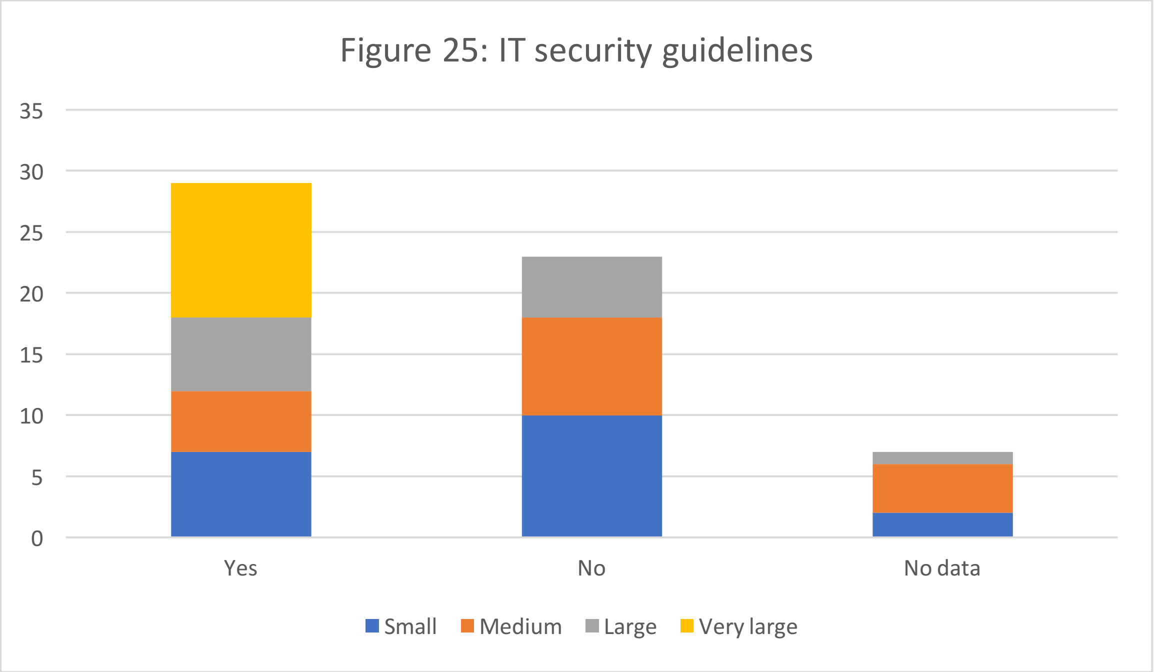


Figure 25: Are there recorded IT security guidelines for the energy control system in your company?

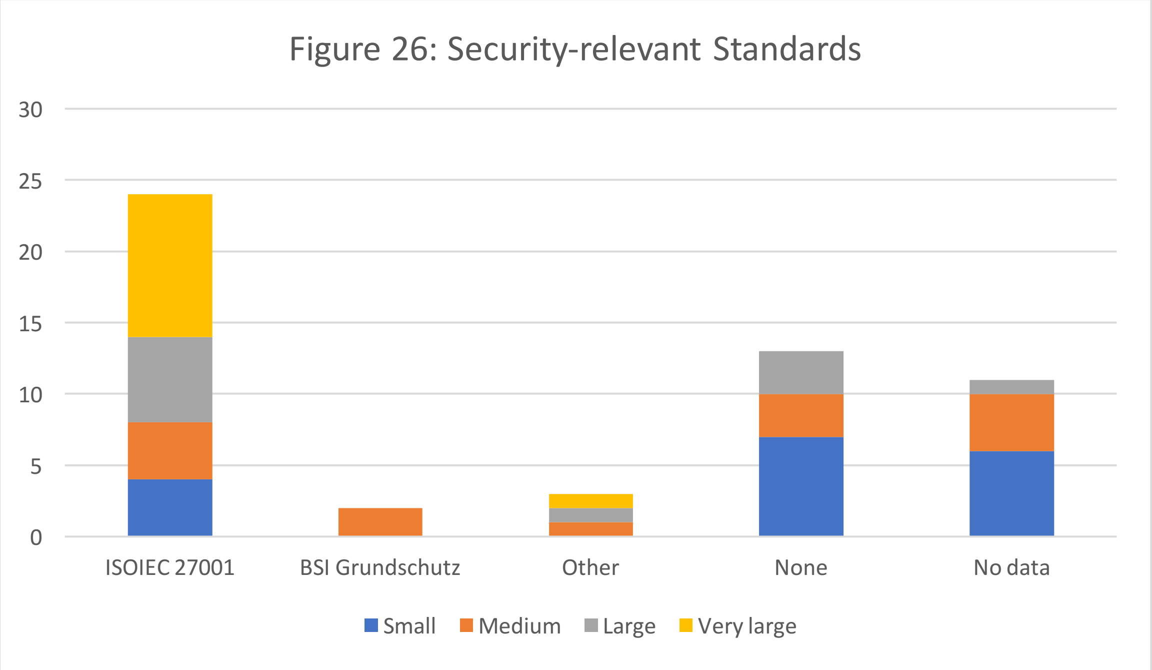


Figure 26: Under which security-relevant standards are your IT systems and processes for network administration elaborated?

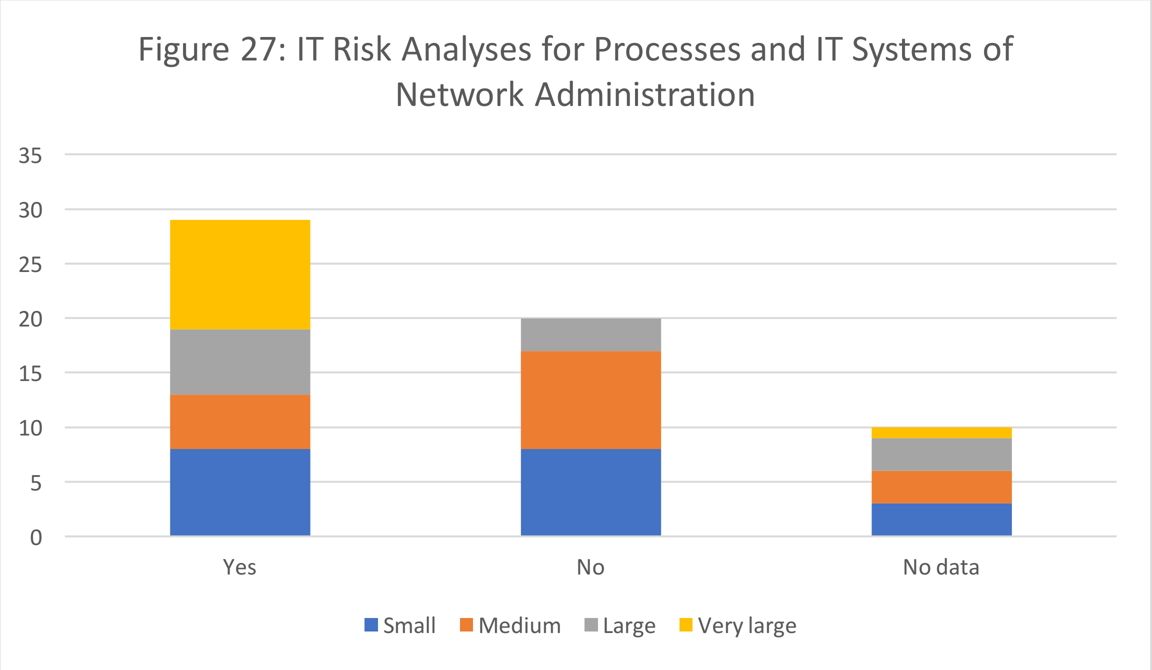


Figure 27: Do you perform IT risk analyses for the processes and IT systems for network administration?

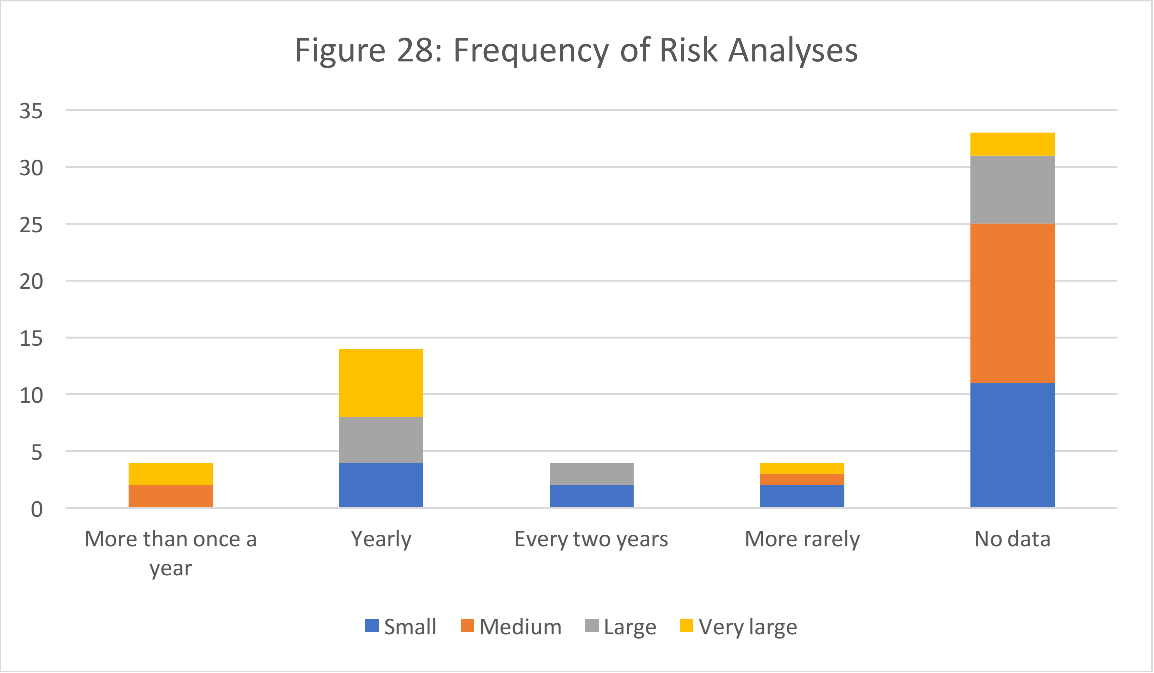


Figure 28: How often do you perform such risk analyses?

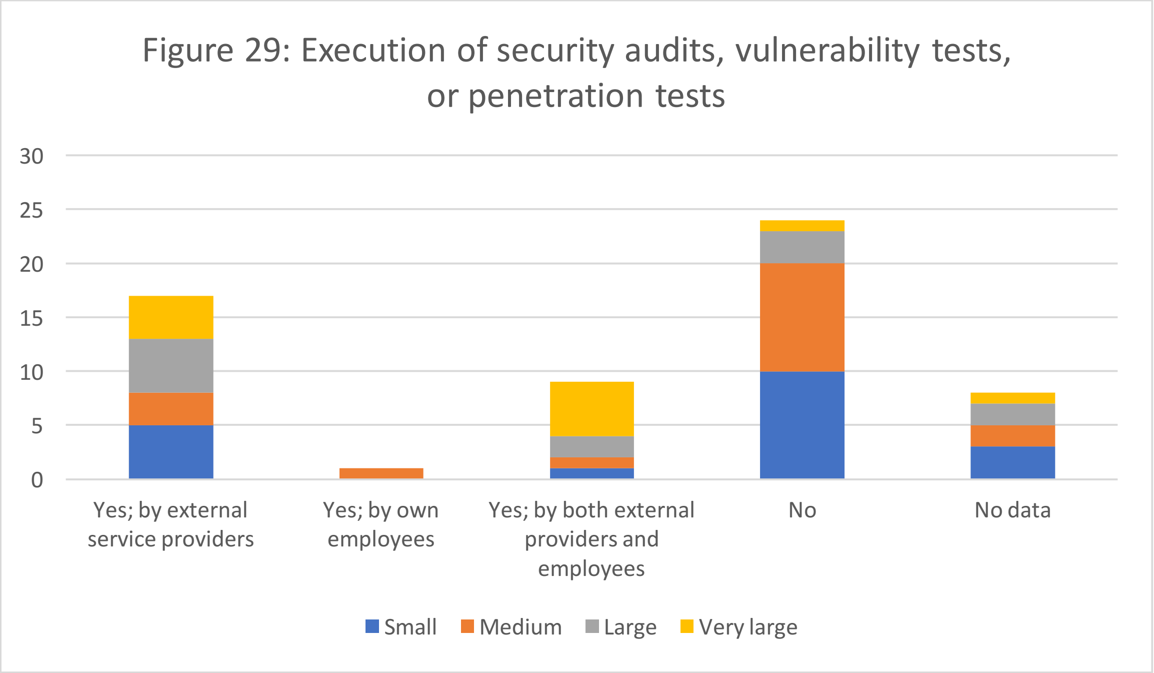


Figure 29: Do you perform security audits, vulnerability scans, or penetration tests for the administration systems of the network management technology?

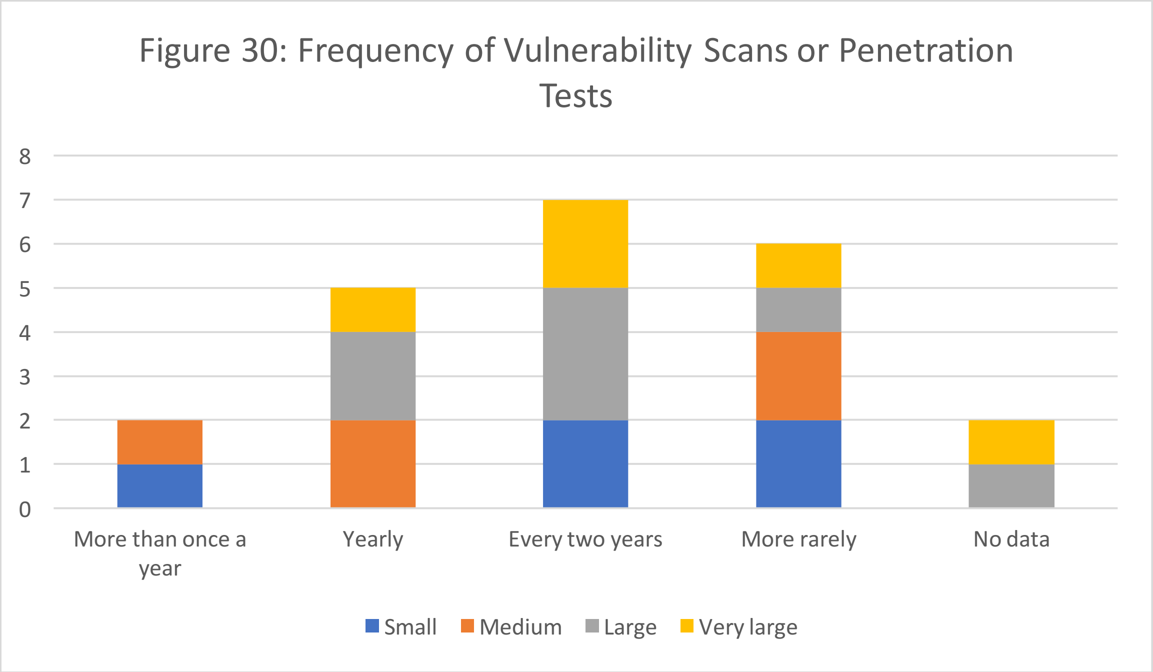


Figure 30: How often do you perform such vulnerability scans or penetration tests?

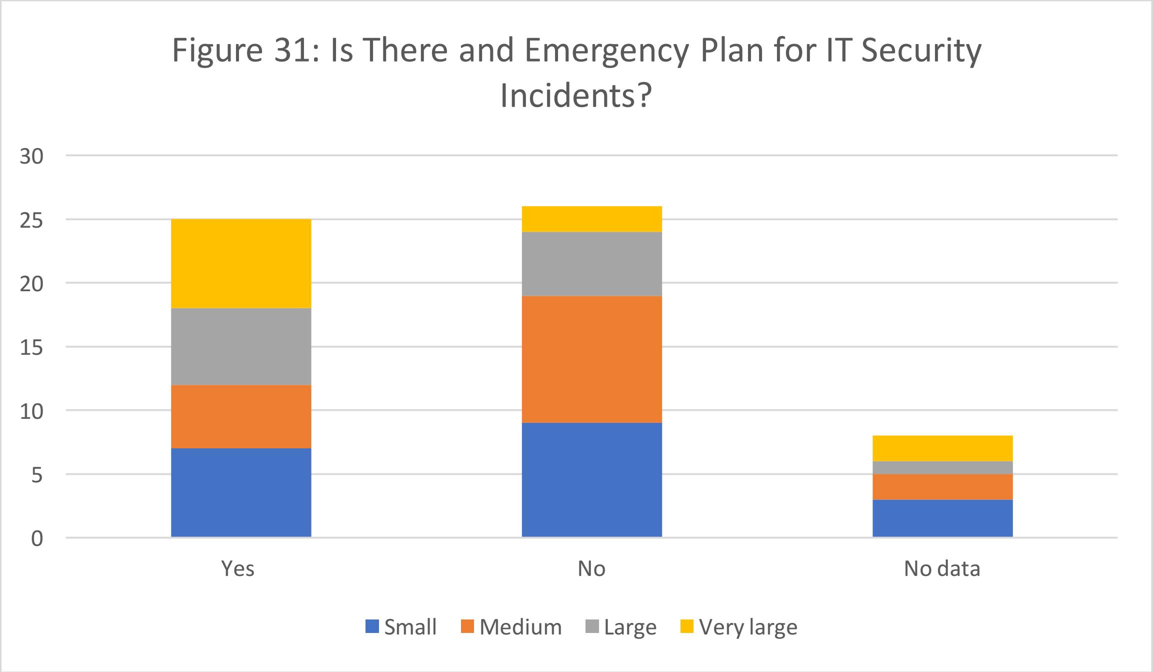


Figure 31: Do you have an emergency plan for security incidents of network administration?

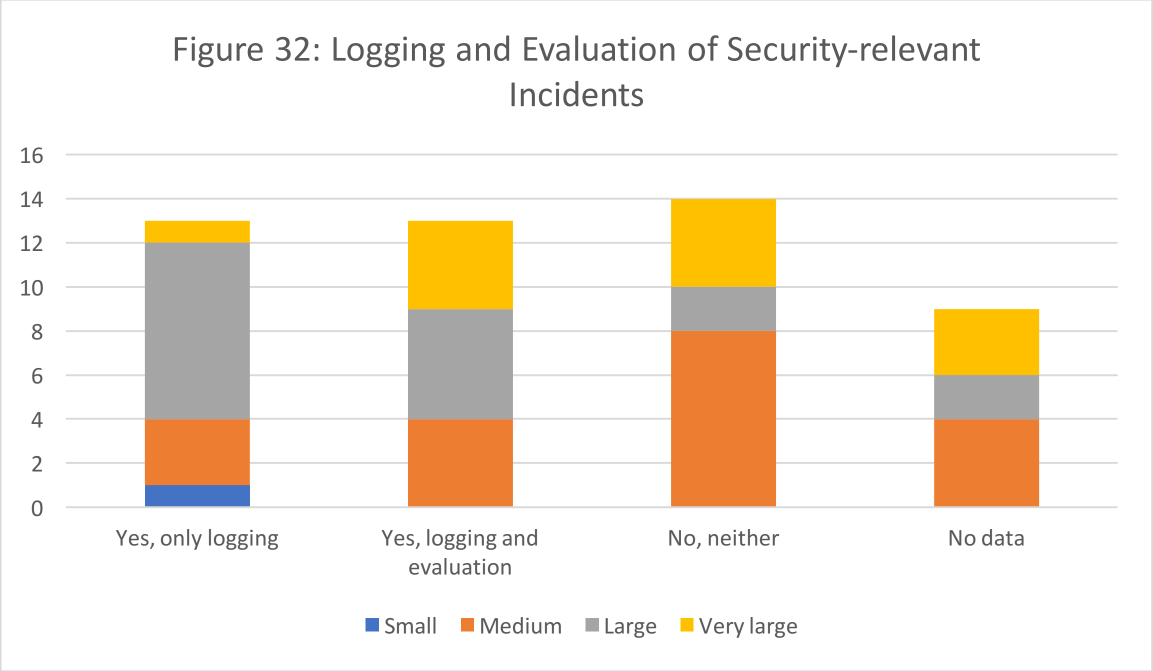


Figure 32: Are security-relevant incidents (e.g. portscans, failed login attempts, unauthorised processes) recorded and evaluated?

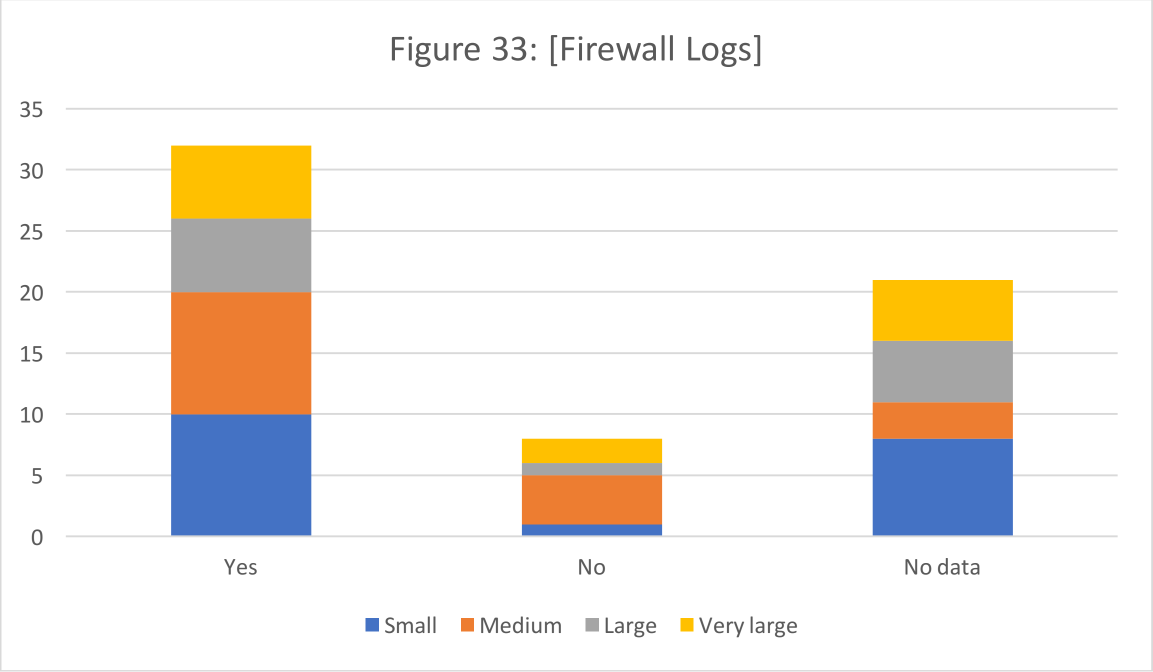


Figure 34: [System Logs]

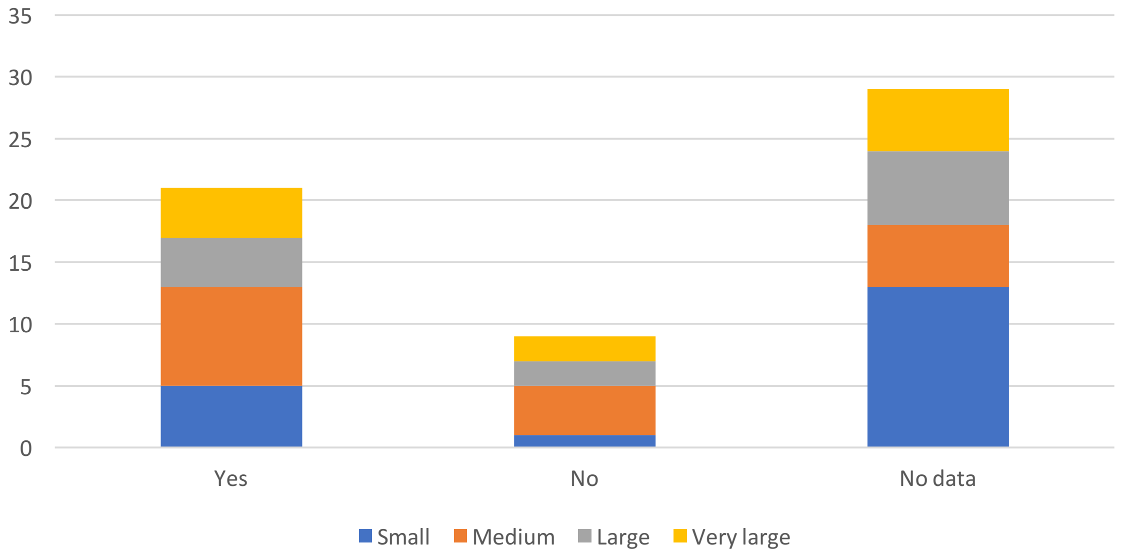


Figure 35: [Failed Logins]

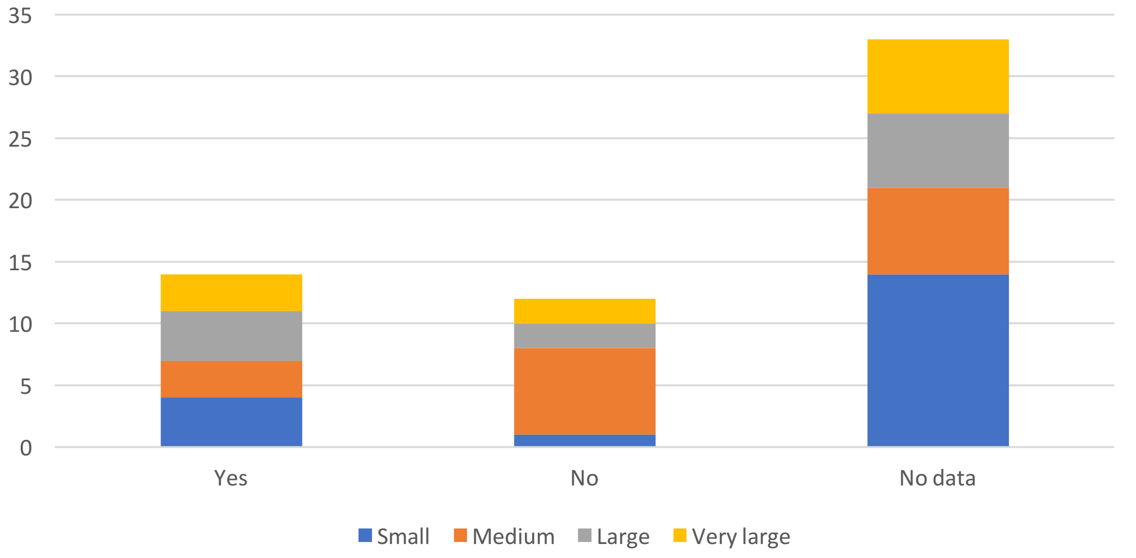


Figure 36: [Honeypot Logs]

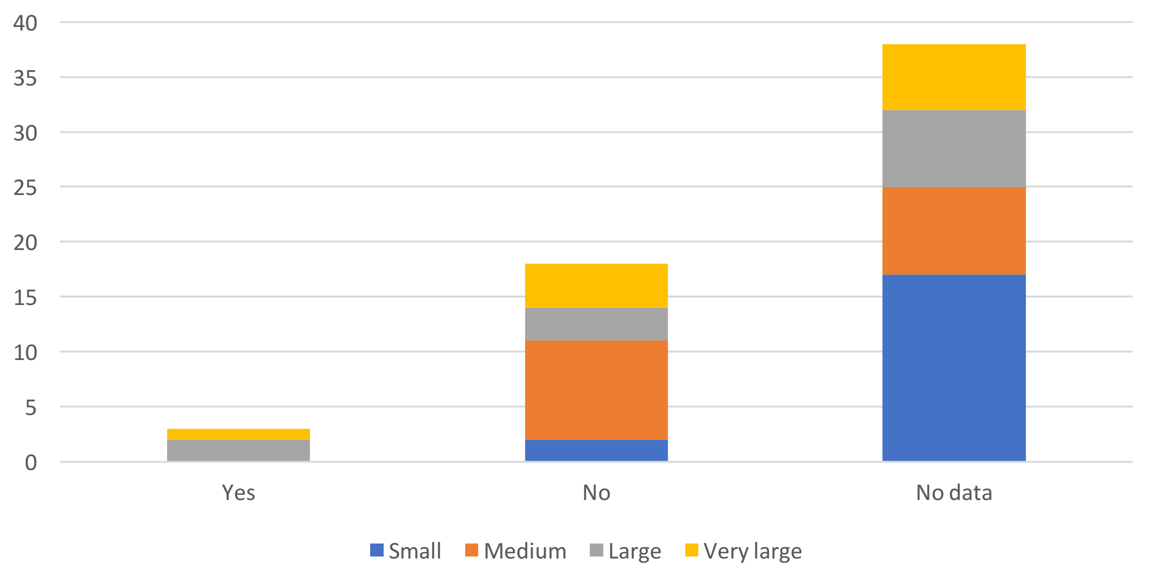
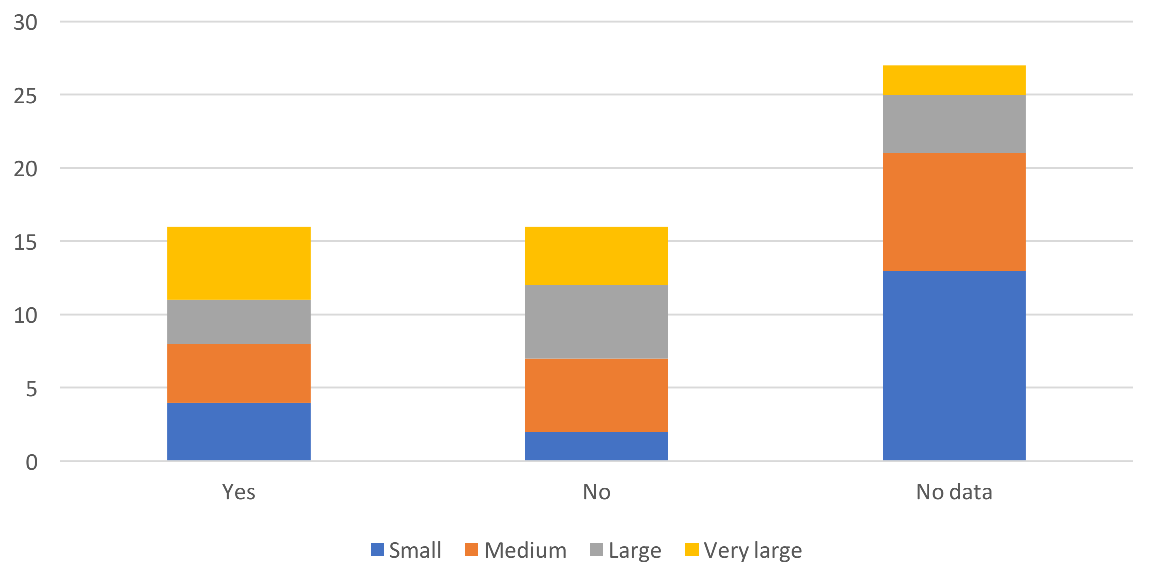
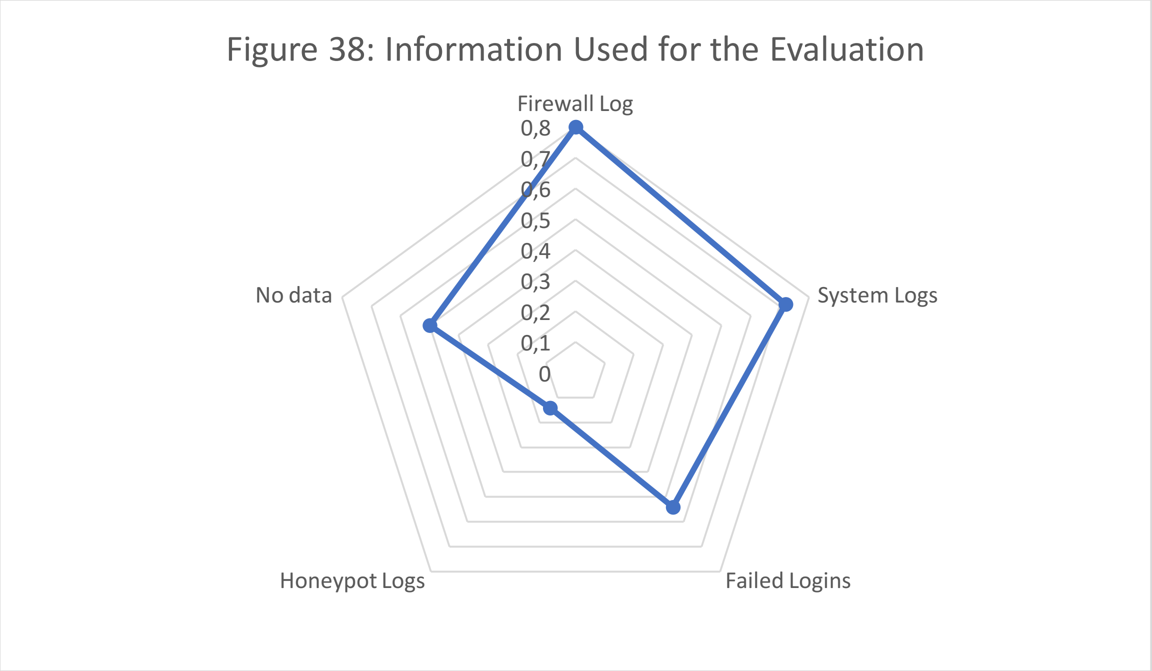


Figure 37: [No data]





Figures 33 to 38: What information do you evaluate for identifying attacks in your IT systems for network administration? (Multiple selection possible)

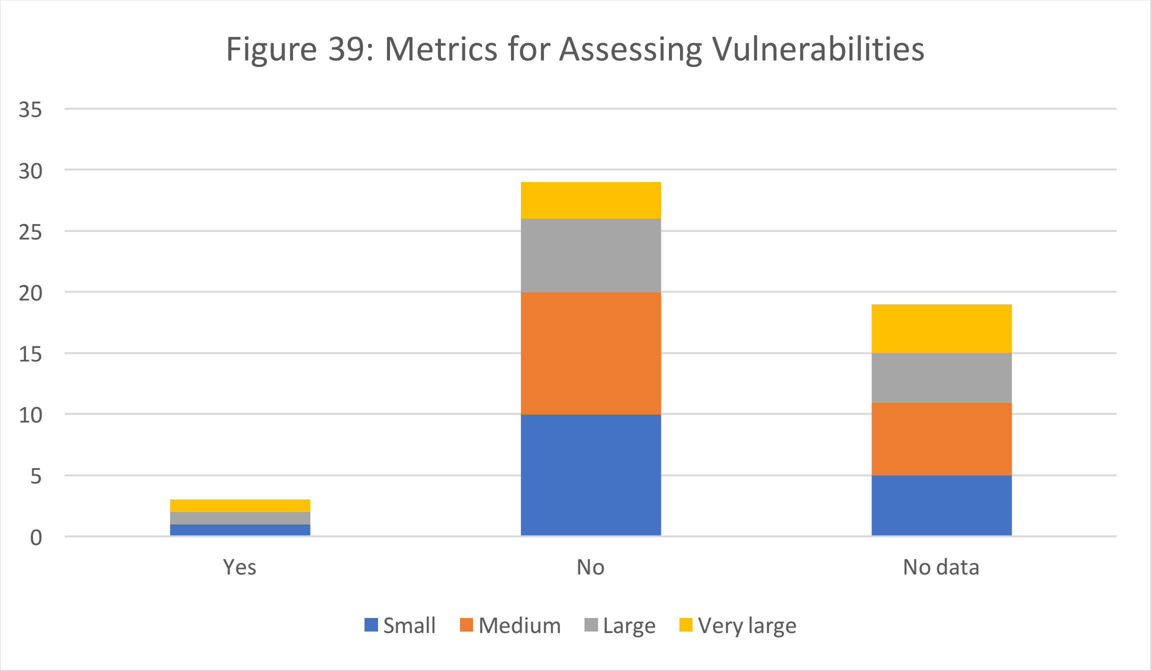


Figure 39: Do you use metrics to assess vulnerabilities (e.g. CVSS)?

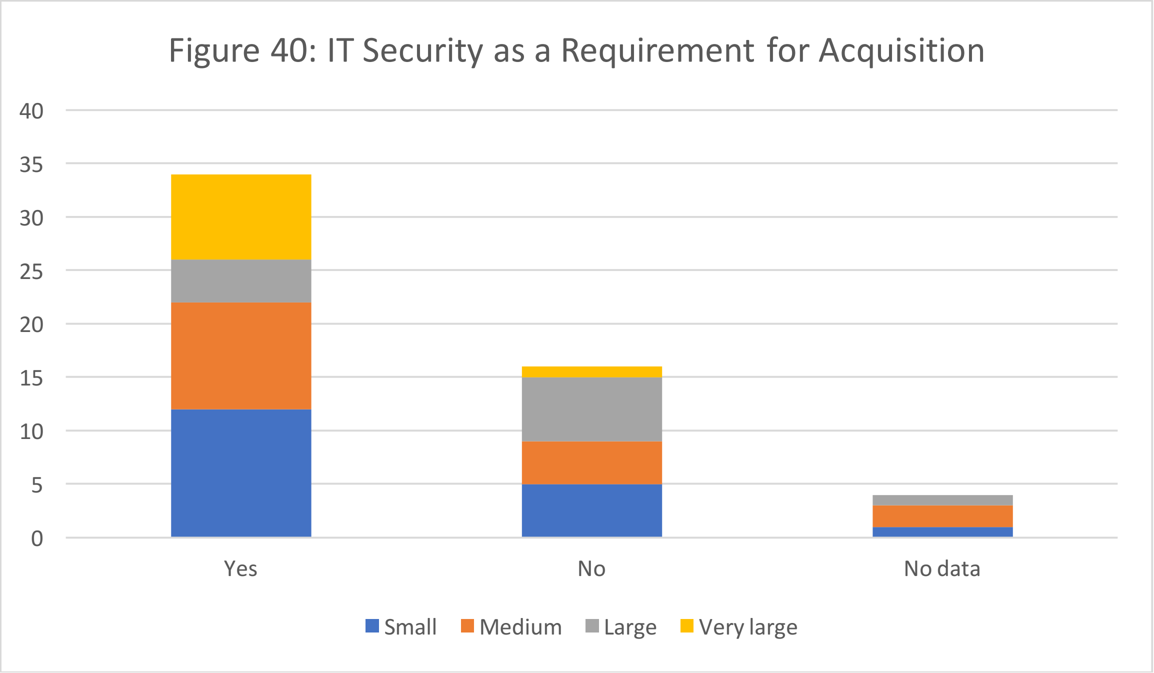


Figure 40: Is IT security defined as a requirement for acquiring new hard- and software?