Analysis of security measures deployed by e-communication providers

DECEMBER 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA's Article 13a Experts Group

ISBN: 978-92-9204-205-9, doi: 10.2824/074677

Table of Contents

Executive Summary

It is of utmost importance that providers of electronic communications take appropriate measures to address major security concerns.

In this concise document the focus is on security measures the providers of electronic communications have deployed to protect their networks for the provision of services, but equally important, the personal and operational data of their customers.

The inputs for this report were obtained directly from providers by means of a survey and a few accompanying interviews. The providers were asked to assess to what degree they have implemented measures earlier recommended by ENISA.

Some of the main findings are the following:

- The majority (63%) of providers have detailed information security policies in place that are reviewed periodically. The documented security policy does not necessarily mean that there is a single and comprehensive document for security policy.
- Quite a high number of 60% of providers can differentiate between security incidents caused internally and those caused by third parties.
- The basic level of access control is implemented by the vast majority of electronic communication providers. However, there is a discrepancy between having the policy document and effectiveness of its implementation.
- The European providers generally display a high operational maturity having personnel assigned with responsibilities for key network and information systems. However, there is still room for improvement about keeping a proper documentation and tracking of incidents on the critical systems.
- Intrusion detection systems are the most widely used incident detection capabilities with 67% of providers having them in place.
- While 88% of operators communicate and report incidents to third parties (government, customers), only 50% have documented policies on incident reporting.

All-in-all, most of the providers report a very good level of using ENISA recommendations on security requirements, while virtually all providers have deployed a good level of basic security controls. In some security domains, the level of maturity reported is high as well as the sophistication of implemented controls. Security of systems and facilities is an example of a security domain with a relatively high maturity of measures adopted. For other domains, though, there is an ample room for improvement, and in particular, the availability of specific policies and operational documentation is lower than desired.

A key conclusion is that while all IT security basics are covered, the achievement of the next level of maturity is impeded mostly by lack of sustainability mechanisms, i.e. repeatable processes and the regularly maintained documentation.

The main recommendation for the providers based on the reported deployment of security measures is to pay additional attention to sustainability and efficiency. This is best achieved by the adoption of Service Management frameworks and creating a series of processes that include measurement and periodic reviews of security controls and capabilities in all domains.

- All security controls are subject to degradation due to either threat advances, i.e. new exploitation techniques like Zero-day vulnerabilities, or due to system configuration changes that happen for reasons of software upgrades, additional business functions assumed by the same information systems, personnel changes, etc. The way to ensure the efficiency of security control is the introduction of periodic review and testing. Data collected from the surveys support the conclusion that little effort is directed to periodic verification of the controls efficiency.

- To support and facilitate the developments of the above it is recommended to adopt management frameworks. The most common service management framework used by many e-communication providers worldwide is ITIL[1]. In particular, Continual Service Improvement (CSI) is suggested for adoption if adopting the whole framework is not a business viable option. CSI process is designed to improve the effectiveness and efficiency of IT processes and services, and can be easily expanded to cover security-related processes.

[1] Information Technology Infrastructure Library, is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL V3), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage. More info are available here: https://www.axelos.com/best-practice-solutions/itil

1. Introduction

New regulatory requirements in the area of security and integrity of networks have been introduced in 2009 by the Article 13a of the Framework Directive. On 14 September 2016 The European Commission presented a draft of the legal overhaul of the telecoms regulatory package. The proposed Directive establishing the European Electronic Communication Code brings also changes to the Article 13a, which is in the draft numbered as Article 40 under the heading "Security of networks and services".[2]

In order to support the implementation of the Article 13a, ENISA has set up a group of experts comprising National Regulatory Authorities (NRAs) from EU Member States plus EFTA countries. ENISA has also established a reference group of experts from within providers of electronic communication networks and services which serves as a forum for discussing their experience, ideas as well as ENISA draft reports.

1.1 Objectives of the report

The aim of this document is to provide an overview of good practices as regards security measures that are deployed by electronic communication providers in Europe. In particular, the document aims to:

- Identify the implemented security measures and approaches within e-communication providers in order to mitigate the main types of incidents in the telecommunications sector and align the findings with earlier ENISA work in this area;
- Identify lessons learned from the above mentioned practices, security measures and approaches;
- Identify security measures and approaches other than proposed by ENISA;
- Issue recommendations and good practices for e-communication providers.
- Provide support to NRAs and policy makers for tracking progress on security measures adopted and for regulatory improvements.

1.2 Target audience

The intended target audience for this document are especially the electronic communication providers and the National Regulatory Authorities (NRAs). Both categories of stakeholders will get an overview on how much the providers have progressed in implementation of security measures in individual security domains. The document will provide support to NRAs as regards areas where they need to try to encourage or commit providers to take more action. While not in every EU country electronic communication infrastructure is labeled as critical, the protection of such infrastructure should be of utmost importance. Constantly evolving threats and risks, if not directly targeting the communication infrastructure, use it as a media to access infrastructure parts that have been labeled as parts of European Critical Infrastructure (ECI). As important stakeholders NRAs strive to improve overall security practices among electronic communication providers.

[2] https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code

Last but not least the document may be useful also for policy makers at the level of the EU and the Member States while preparing the review of the existing telecoms regulatory package.

1.3 Previous work undertaken by ENISA

ENISA has commissioned a number of reports and documents relating to the topic of security measures. Among these, the following are the most significant:

Technical Guideline on Security Measures (version 2.0., October 2014)[3] This document serves as a guidance to NRAs on the implementation of Article 13a and in particular on the security measures that providers of public communications networks must take to ensure security and integrity of these networks. The document lists the minimum security measures NRAs should take into account when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

Guideline on Security measures for Article 4 and Article 13a[4] - The document provides a guidance to national competent authorities about the supervision of security measures in Article 13a of the Framework Directive (2009/140/EC) and Article 4 of the e-Privacy directive (2002/58/EC). In particular, it lists security measures national competent authorities should take into account when evaluating the compliance of public communications network and service providers with paragraph 1 of Article 4 and paragraph 1 and 2 of Article 13a.

Technical Guideline on Threats and Assets[5] - The document provides NRAs with a glossary of terms to communicate about the most significant threats and network assets involved in disruptions in electronic communications networks and services. The threats and assets described in this document are based on past incidents, as reported by the NRAs to ENISA and the European Commission.

Impact evaluation on the implementation of Article 13a incident reporting scheme within EU[6] - The document aims to assess the real impact of the Article 13a. The evaluation focused on five key areas: the new security measures implemented in the member states, the transparency resulting from the incident reporting process, the learning process resulting from incidents, the level of collaboration between the stakeholders and the harmonization of the procedures within the European Union.

1.4 Methodology

Two main tools were employed in this project to become familiar with the security measures of the e-communication providers, an online survey and accompanying interviews with some of the providers who have already responded to the survey. The aim was to get insights into how the providers assess their own level of achievements in implementing the recommended set of security measures.

1.4.1 Online Survey

A survey consisting of 20 questions was commissioned for the delivery of this document. The core of the survey was based on earlier ENISA documents relating to security measures, especially on the list of security domains, objectives and measures and the level of sophistication of the measures. The document Technical Guideline on Security Measures mentioned above includes a list of 25 security objectives grouped in 7 security domains while each objective lists the respective security measures to reach the

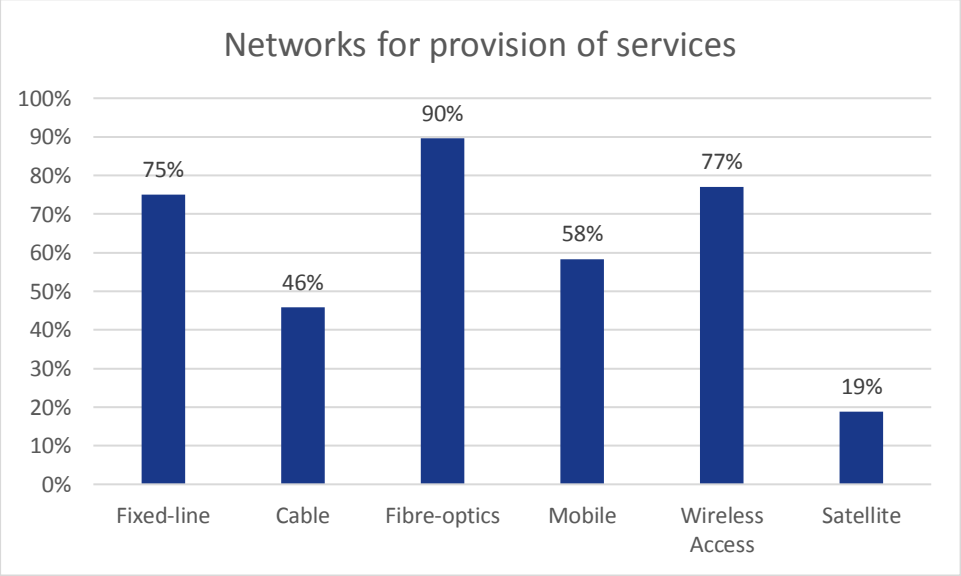
[3] https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures
[4] https://www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a
[5] https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets
[6] https://www.enisa.europa.eu/publications/impact-evaluation-article13a

security objectives (see Annex A:). The security measures are categorized into three levels of increasing sophistication. This categorization was also used for the survey, which was conducted for this report. The respondents were asked to attach sophistication levels to the security measures implemented. Not all the security objectives and measures were included in the survey to keep it concise and manageable for the respondents.

For most of the questions respondents were asked about the perceived level of sophistication (implementation) of these measures. All main security objectives were covered by the survey apart from Human resources security which was partly grouped with Governance and risk management. To keep the survey concise and manageable for the respondents, not all of 25 security measures were included. On the other hand, the survey touched upon specific measures against DDoS attacks, for SS7 protocol as well as upon the security standards followed. For most of the questions the respondents had the option to provide further details and clarifications.

The respondents included electronic communication providers from Europe, the vast majority of them being from the EU Member States. The pool of respondents came from ENISA and their contractor's contacts among providers. The survey was conducted in the summer months of 2016. In total, 48 European providers responded to the online survey. The sample consisted of a variety of operators and Internet service providers, the most of which provide their services over both fixed and mobile networks. Their networks are rather sophisticated and the majority of them claims to have deployed fibre optics. The main findings of the survey are analysed in the following chapter **Error! Reference source not found.**.

Figure 1: Networks used for provision of services by the operators surveyed



1.4.2 Interviews

While the survey generated a good overview of the measures adopted and their perceived level of sophistication, it was complemented by several interviews with selected stakeholders. The aim was to better understand the rationale behind the approaches of individual providers and gather insights into other areas not properly covered by the survey. The interviews were either conducted in person or via electronic means while the interviewees had received the questionnaire in advance

1.5 Structure of the report

Chapter 2 provides in its charts and commentaries a more detailed overview of implemented security measures, which is the core of this document. These measures are aligned according to the list of security domains and objectives present in earlier documents of ENISA (see **Error! Reference source not found.**). In ost cases, the sophistication of these measures is identified. The security domain of Human resources security was loosely aligned with Governance and risk management and not all of security objectives (measures) were subject of this exercise.

Chapter 3 draws conclusions on the findings and suggests areas for improvements and further steps to be taken by the providers. Per each security domain a conclusion is drawn (on a three-grade scale) as regards the maturity of the measures implemented. This chapter also includes some recommendations for the providers of electronic communication.

2. Security measures adopted: status and level of sophistication

This chapter analyses the security measures adopted by electronic communication providers drawing on the results of the survey and the accompanying interviews. It focuses mostly on the level of sophistication (usually three-grade scale) of these measures as perceived by the operators. The security measures are mainly introduced to protect the main assets of the operators, which are private and traffic data of customers and the infrastructure that enables the provision of services. At the same time, anything that impacts and threatens (the integrity) of customer data is considered as one of the main risks and threats as the reputation of the company may be seriously damaged. As mentioned earlier, the structure of security domains and security objectives from earlier ENISA documents serves as a basis for the analysis with a few additional topics that are treated independently from the original list of security domains and objectives. These additional topics are the compliance with international security standards and practices as well as security measures employed against DDoS attacks and for SS7 protocol.

In the following analysis, we refer to sophistication levels of the measures. These broadly correspond to three level applied in earlier ENISA documents and are cumulative, i.e. the level 2 includes all features of level 1 and level 3 includes all features of levels 1 and 2.

Sophistication level 1 (basic):

- Basic security measures that could be implemented to reach the security objective.
- Evidence that basic measures are in place.

Sophistication level 2 (industry standard):

- Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents.
- Evidence of industry standard measures and evidence of reviews of the implementation following changes or incidents

Sophistication level 3 (state of the art):

- State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures.
- Evidence of state of the art (advanced) implementation, evidence of a structural review process, and evidence of pro-active steps to improve the implementation of security measures

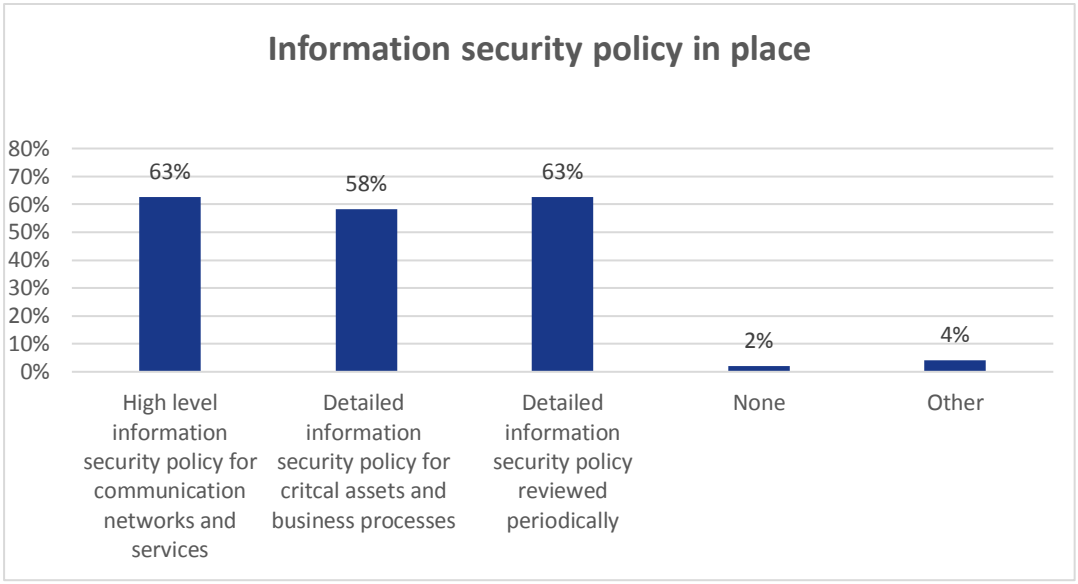
2.1 Governance and risk management

2.1.1 Information security policy

The information security policy is the first security objective covered by the above mentioned “Governance and risk management” security domain. Almost two thirds of the operators claim they have reached the third (highest) level of sophistication, i.e. that they have detailed information security policies in place that are reviewed periodically. That could either mean that they consider their own information security policies to be up to date and approved by senior management and/or that the review process is

documented taking into account violations, exceptions, past incidents, past tests/exercises as well as incidents that affect other providers in the communications sector.

Figure 2: Information security policies as applied by European operators



While policy reviews indicate a higher information security maturity within the providers it is unclear why the high-level policy number is relatively low. The high-level policy is a document stating information security requirements for the organization at a corporate level and it is a key element of security governance. The upper level document is usually followed by a series of more specific policies. There is a number of public resources that can aid providers in creation of not only high level but also specific policies. [7] [8]

The documented security policy does not necessarily mean a single and comprehensive document for security policy. For example, one operator confirmed that they have specific information security policies for information classification/management, access management, secure development of applications and services and secure infrastructure Implementation. As regards the review of security policies, this includes, for example, the evaluation of the current information security policies in line with the framework of the ISO 27001 standard.

For the implementation of appropriate security policies the operators need to have a skilled work force at their disposal. Usually the security roles are divided between separate divisions managed by CTO or CSO, while very rarely there are only IT-security specific roles. Some operators have established security committees (with their members coming from various departments) that oversee the implementation of security policies. As regards the enhancement of IT security skills of employees, they often receive e-learning trainings on password policies, malware etc.

[7] https://www.sans.org/security-resources/policies/
[8] http://www.dmoz.org/Computers/Security/Policy/Sample_Policies/

2.1.2 Risk management

The list of risks is an effective way to raise management awareness so they can make established acceptable risk levels and quantities. Risk lists can be decentralized i.e. maintained by respective departments of the provider if the central risk management function is not established.

Almost two thirds of operators keep a list of main risks for security and continuity of their networks and services and their key personnel is aware of the main risks. A slightly lower share of operators have a documented risk management methodology and tools and periodically review this methodology and tools taking into account changes and past incidents.

Similarly, to the high-level security policy document, maintaining the list of risks is rather a low effort exercise. Ideally, the deployment of risk management measures should be somewhat higher to indicate that risk management receives appropriate attention.

Figure 3: Risk management framework

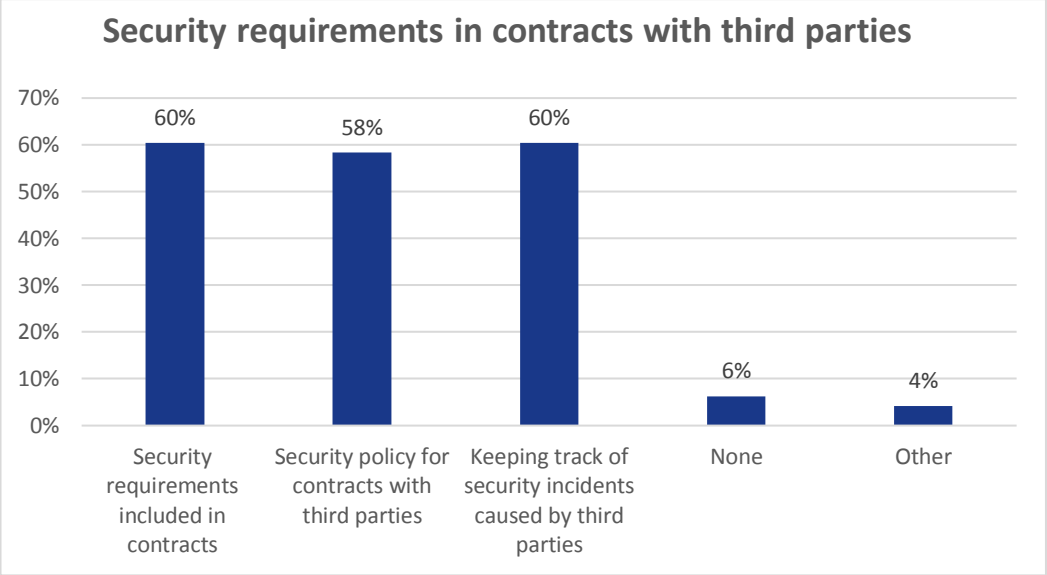
The providers often align business continuity management with security standards like ISO 22301 and BCI (Business Continuity Institute) Good Practice Guidelines. Also, as with the previous topic of information security policies, there are specific tools for different areas (IT or telecommunication network) with different levels of sophistication.

2.1.3 Security requirements for contracts with third parties

The telecommunication providers need to implement a policy on security requirements in order to procure and manage third-party networks and services like, for example, IT services, software, call-centres, shared facilities, interconnections etc.

Around 60% of providers include these requirements into the contracts and maintain and update respective policies while keeping track of security incidents related to or caused by third parties. While there is not much indication on the quality and coverage provided by the third party security policies, the ability of 60,42% of providers to differentiate between security incidents caused internally and externally can be considered as a very good achievement.

Figure 4: Security requirements in contracts with third parties



When deciding whether to include security requirements in individual contracts with third parties, the providers take into account, for example, the criticality of the systems/services or costs. It is important to note that the upcoming General Data Protection Regulation (GDPR)[9] defines the responsibilities for entities that collect personal data (collectors) and process personal data (processors). As many of the eCommunication providers deal with personal data in one or the other way, the GDPR will heavily affect the majority of them. In case their role falls under definition of data collectors, it will be their responsibility to track and inform about data breaches even if they are caused by the contracted third parties.

2.2 Security of systems and facilities

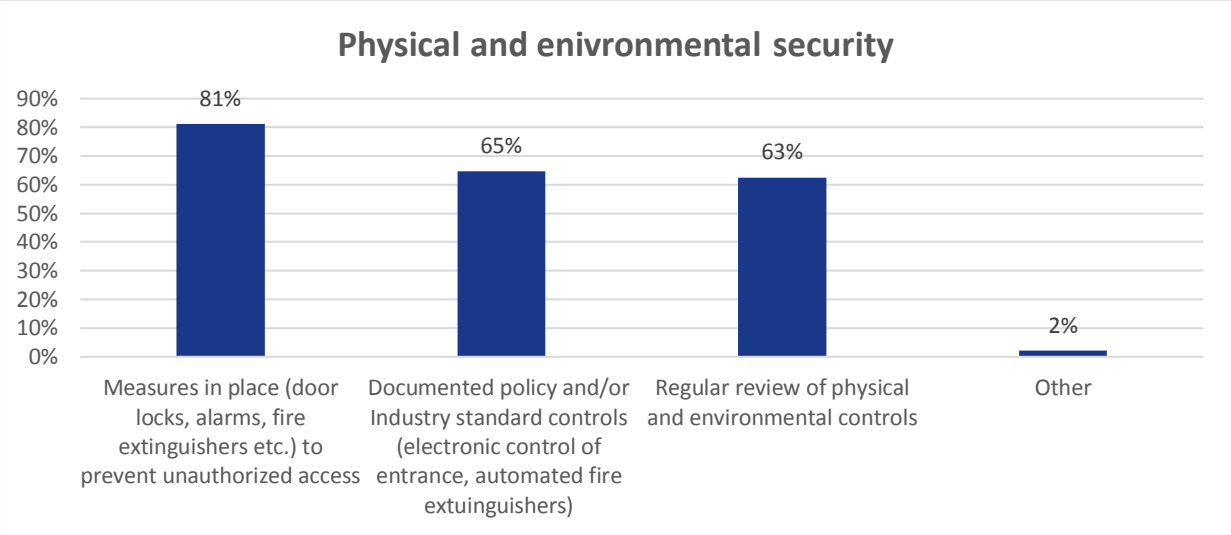
2.2.1 Physical and environmental security of network and information systems and facilities

This particular area relates, inter alia, to the need for the providers to house critical and sensitive information in secure areas and to protect them by defined security parameters along with appropriate security barriers and entry controls. It also means that "physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied."[10]

For example, there are specific rules for building datacenters when the operators need to take into account the surrounding area like the altitude or the close presence of a gas station.

[9] http://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en
[10] ISO27002, Chapter 9.1.4

Figure 5: Physical and environmental security



The vast majority of the providers (more than 80%) have measures in place to prevent an unauthorized access to facilities which includes door and cabinet locks, burglar and fire alarms, fire extinguishers etc. Almost two thirds of them implement a policy for physical security measures and physical and environmental controls including industry standards.

These standards include electronic control of entrance and audit trail, segmentation of spaces according to authorization levels, automated fire extinguishers with halocarbon gases and so on. Also, approximately the same number (62.50%) of providers also evaluate and, when necessary, review and update the policies for physical security measures and environmental controls in the light of changes and past incidents. These figures can be considered as sufficiently high.

2.2.2 Access control measures

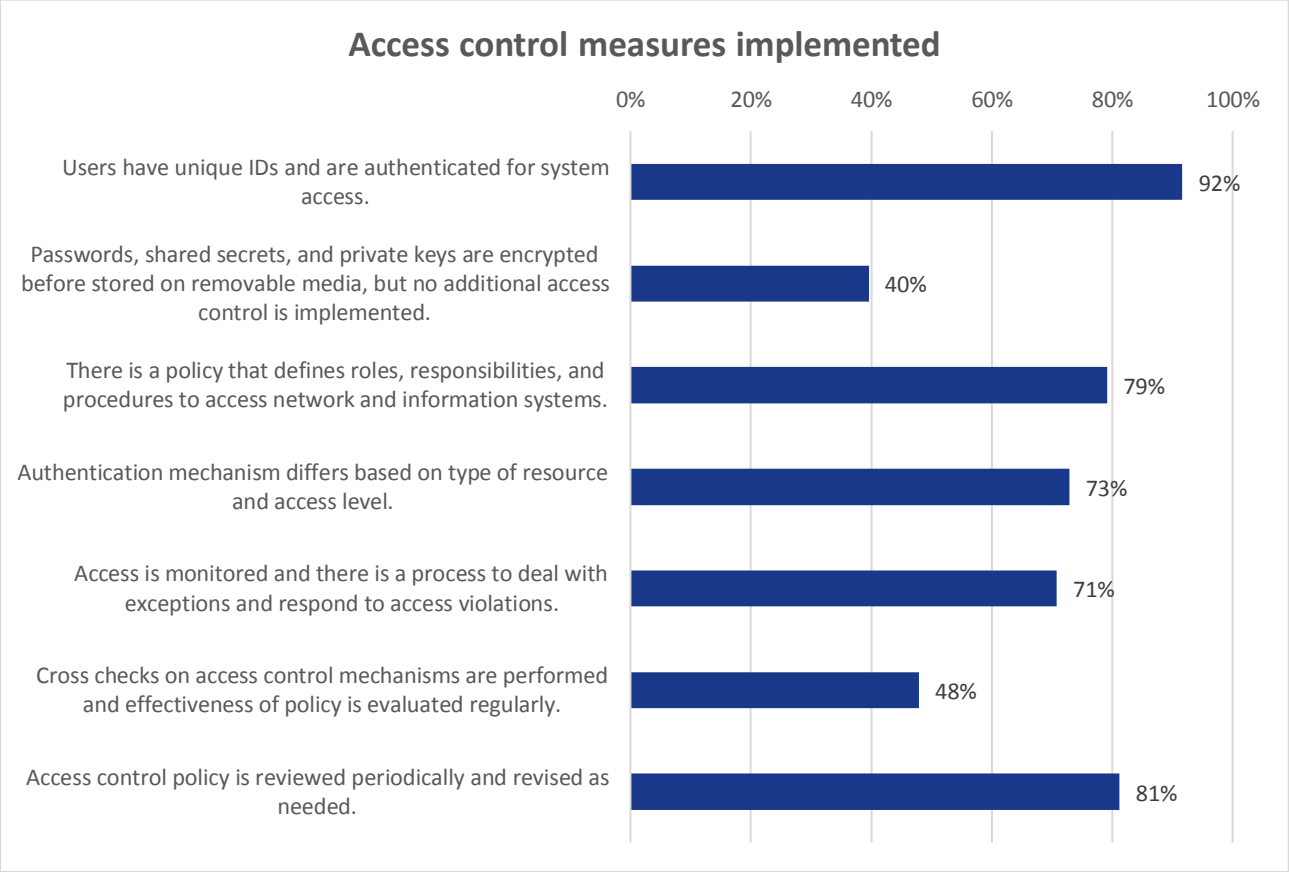
The electronic communication providers should have in place appropriate (logical) access controls for access to network and information systems. This access should be controlled on the basis of business and security requirements. The access control rules are categorized based on the criticality of data and also on their life-cycle (when the data is stored, when it is destroyed).

The first grade (sophistication level) of access control rests with the access logs showing unique identifiers for users and systems as well as an overview of authentication and access control methods for systems and users. In almost 92% cases users have unique IDs and are authenticated for accessing the systems. In around 40% of cases the providers protect passwords using standard cryptographic methods, shared secrets and private keys before storing them on removable media without any additional access control.

The second sophistication level means that the providers have an access control policy in place including description or responsibilities, groups, access rights and procedures for granting and revoking access. Also, different types of authentication measures exist for different types of access. There is also a log of access control policy violations and exceptions which is approved by security officers. Almost 80% of providers claim to have such a policy in place that defines roles, responsibilities and procedures for access to network and information systems. In more than 70% cases the authentication mechanisms differ depending on the type of resource and access level and/or access is monitored and there is a process dealing with exceptions and responding to access violations.

The most mature handling of access controls is to evaluate the effectiveness of access control policies and procedures and to review and, if needed, to revise them. Slightly less than a half of providers are doing cross checks on access control mechanisms and more than 80% of providers review the access control policy periodically.

Figure 6: Access control measures



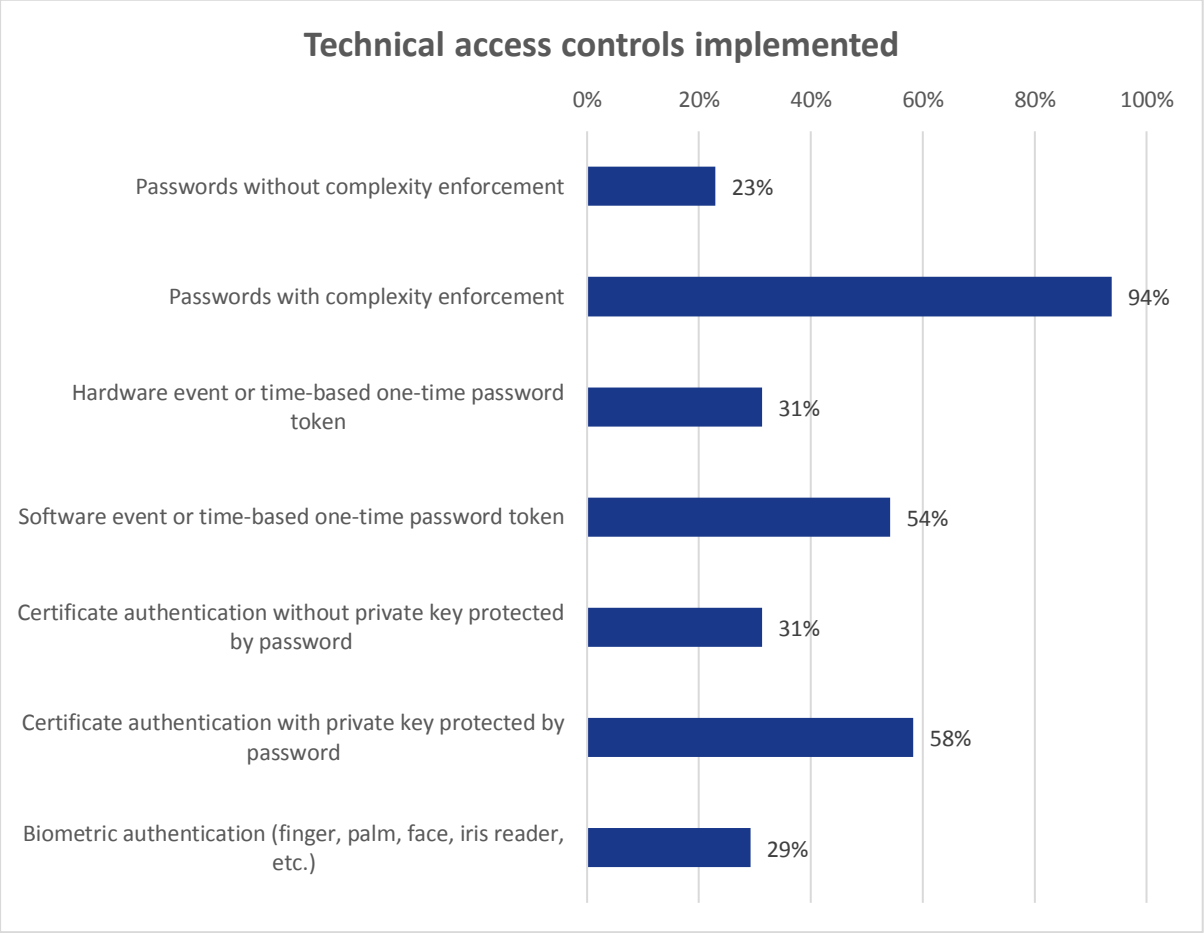
The basic level of access control is implemented by vast majority of electronic communication providers. However, there is a discrepancy between verifying the policy document and effectiveness of its implementation. Checks on access control effectiveness should be stated in policy and executed at least as often as access control policy review itself.

The following figure gives more detailed technical insights on the access controls implemented. The figure covers both low-profile and high-profile security measures. It shows, for example, surprisingly quite a high share (more than 58%) of operators claiming to implement certificate authentication with private key protected by password, while over 31% go without password protection for the certificate authentication. It is important to highlight the significant use of biometric authentication technology that was reported by 29.17% of eCommunication providers.

Responses of the surveyed and interviewed operators on the alignment of the technical access controls with access control policy indicate a comparatively high maturity of the access control measures implemented. A relatively wide use of biometric technology for authentication confirms that conclusion. While the use of certificates without password protection can be explained by operational needs and no password complexity enforcement by limited capabilities of embedded OS on the communication

equipment, both of these areas should be marked for improvement. And while the technical capability to enforce password complexity may not be available on specific devices, the policy should clearly state the access control security requirements[11]. Fulfilment of these requirements should be verified regularly.

Figure 7: Types of access control measures implemented



2.2.3 Integrity of network and information systems

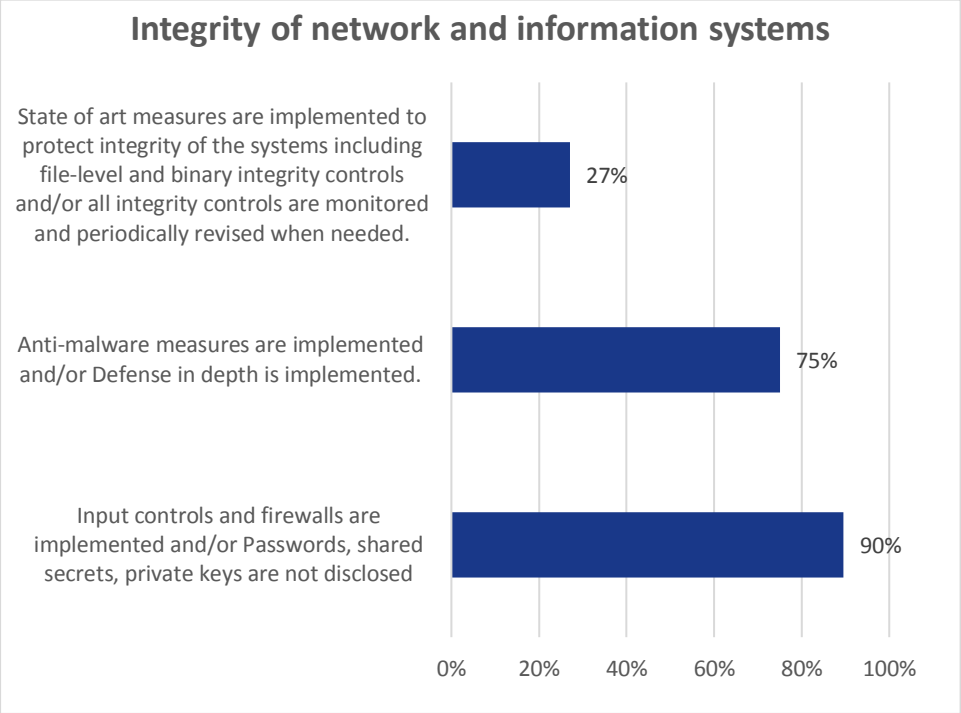
The measures concerning integrity of network and information systems are those that provide protection against malware, viruses and other common threats that can compromise the functionality of the systems. Nine out of ten surveyed operators have implemented the basic level of integrity. That means that software and data in network and information systems are protected by input controls, firewalls, encryption and signing. Security critical data are protected by separate storage, encryption, hashing etc. and malware detection systems are in place and they are up to date.

The second stage of maturity of measures in this area concerns proper documentation of software and data in network and systems, availability of tools for detection of anomalous usage and behaviour of systems and logs of intrusion detection and anomaly detection systems. 75% of operators have deployed these mechanisms to detect whether the network or information systems have been tampered with or altered.

[11] https://www.sans.org/security-resources/policies/general#password-construction-guidelines

State of the art measures, which are the highest on the sophistication scale, are implemented by 27% of operators. These measures aimed at protection of the integrity of the systems include file-level and binary integrity controls. Also, integrity controls are monitored and evaluated for effectiveness and revised if needed. The controls may not be in place in all systems - depending on risk assessment.

Figure 8: Integrity of network and information systems

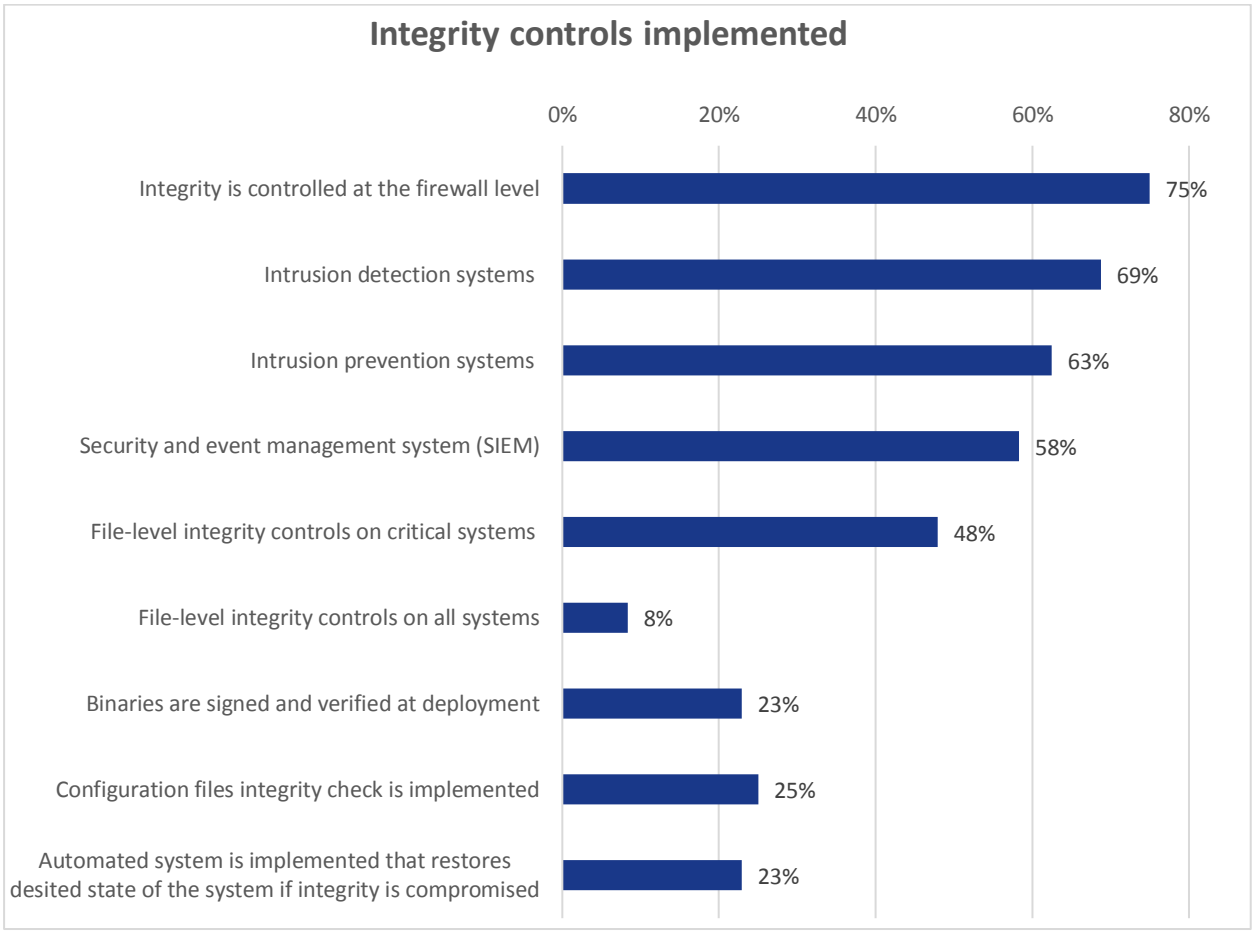


The integrity controls implemented range from basic ones like firewalls to automated restoration of the system desired state in a case the integrity being compromised. Some 75% of operators have integrity controlled at the firewall level, while almost 69% have implemented intrusion detection systems and 62,5% have intrusion prevention systems in place.

In addition to that it is worth noting a relatively high level of implementation of file level integrity controls on critical systems (48%), while the SIEM implementation could be highlighted as the main area for improvement. There is a discrepancy between implementation of configuration files integrity (25%) and file-level integrity controls on critical systems (see above).

Some 23% of operators claim that they have deployed automated mechanisms for restoring the systems to the desired level in case their integrity is compromised.

Figure 9: Integrity controls implemented



2.3 Operations management

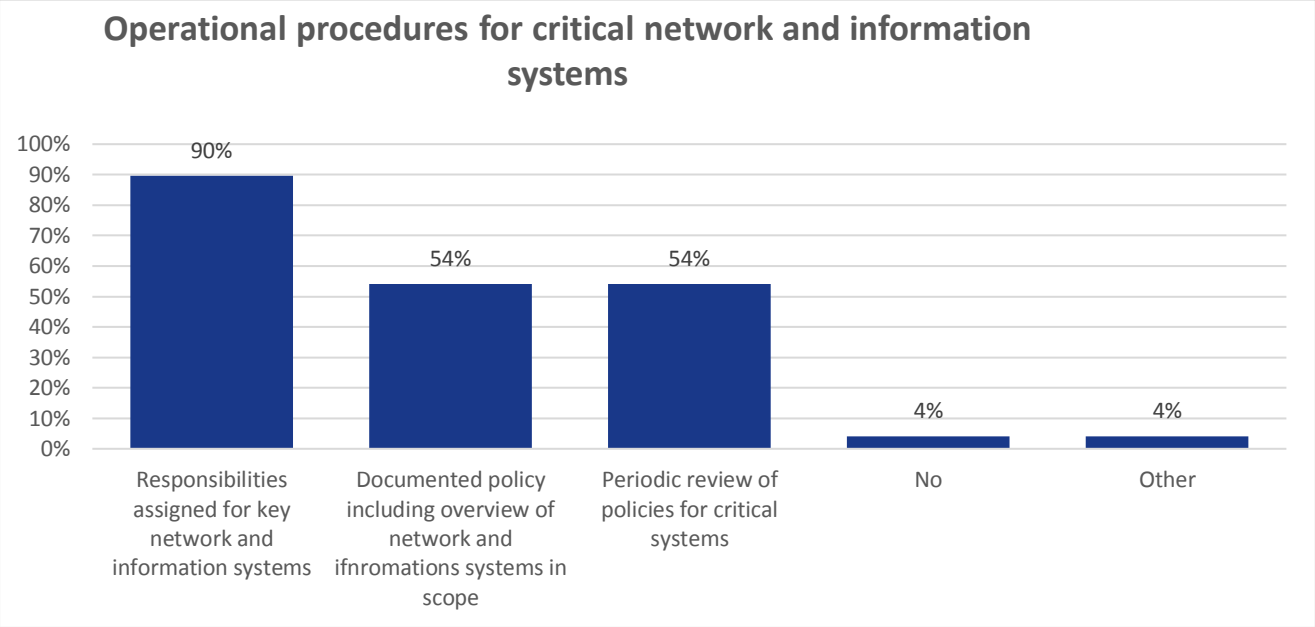
2.3.1 Operational procedures

The providers need to establish and maintain procedures for the management and operation of information processing facilities. The vast majority (90%) of electronic communication providers have assigned responsibilities for key network and information systems.

Over half (54%) of them have introduced respective policies to make sure that all critical systems are operated and managed according to pre-defined procedures. These policies are regularly reviewed and updated. Some providers align the operational procedures with business continuity and information security programs, where critical services and systems are identified.

The European providers generally display a high operational maturity having the personnel with assigned responsibilities for the key network and information systems. However, proper documentation maintenance and incident tracking on the critical systems should be improved.

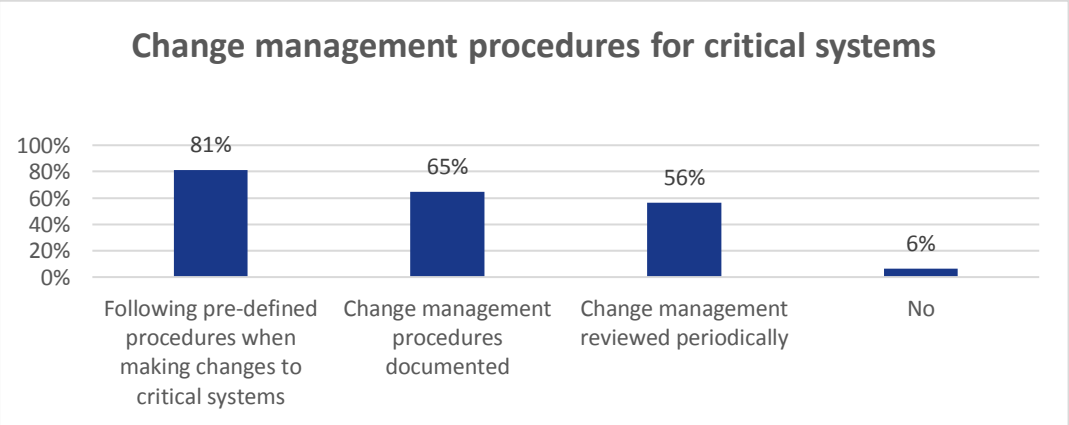
Figure 10: Operational procedures for critical network and information systems



2.3.2 Change management procedures

The change management procedures are established in order to minimise the likelihood of disruptions and errors resulting from the changes. The main goal of change management is to ensure reliable and timely implementation of change requestes with minimal operational efforts. The change management procedure (along with many others) is described in IT Infrastructure Library (ITIL)[12]. According to the ENISA Annual incident report, in 2015 human errors was the root cause category involving most users affected, around 2.6 million user connections on average per incident. Over 81% of providers follow predefined procedures when making changes to critical systems. Around 65% of providers document change management proceduress while these are reviewed by 56,25% of them taking account of changes and past incidents.

Figure 11: Change management procedures for critical systems



[12] https://www.axelos.com/best-practice-solutions/itil

2.4 Incident management

2.4.1 Incident management procedures

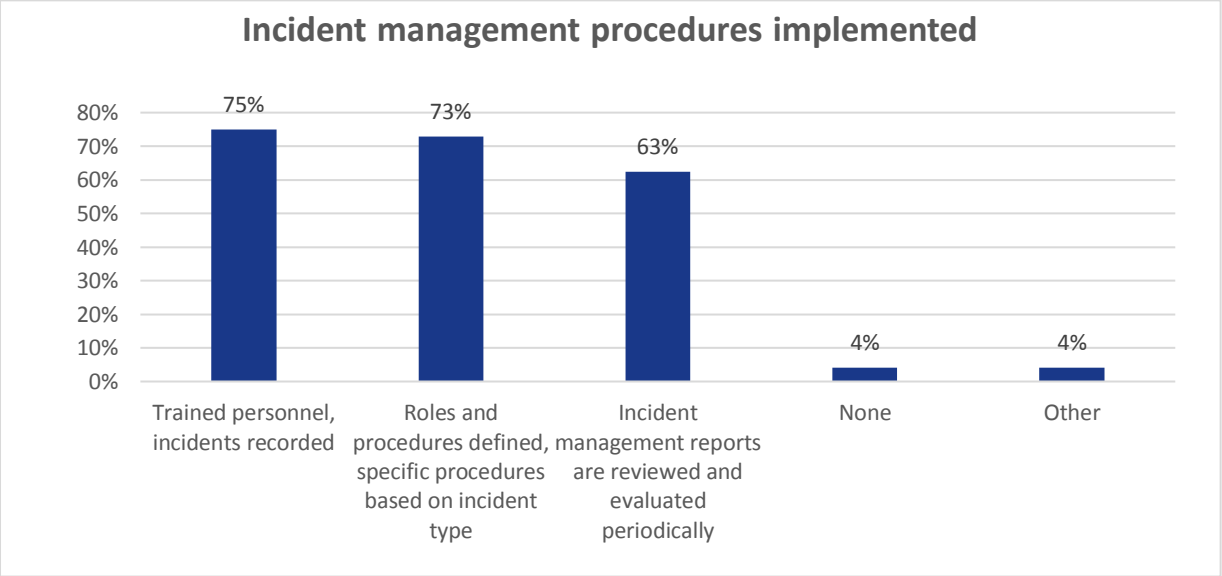
The providers need to have in place and maintain procedures for managing incidents and forwarding them to the appropriate personnel /triage. Advancement of threats and their growing sophistication requires companies to invest in incident management and response in addition to the introduction of preventive measures. Three quarters of the surveyed providers claim that their personnel are trained to be able to respond to incidents and that they record all major incidents.

A slightly lower number (approx. 73%) of providers have developed incident response policies that define roles and responsibilities and contain specific procedures depending on type of incident. Over 62% of providers implement the measures that are highest on the sophistication scale. This means they create incident management reports for all major incidents and they review and evaluate them periodically to update incident management procedures.

Incident management records and reports are created for major incidents when considered relevant. Within the scope of information security, incident management is more mature for continuity-related incidents (more frequent) and less mature for personal data-related incidents (less frequent).

It is interesting to note that the percentage of respondents with more advanced incident management procedures, periodic review and improvement of incident management procedures, roughly corresponds to the number of providers that implemented SIEM and Intrusion Detection/Preventions systems.

Figure 12: Incident management procedures implemented

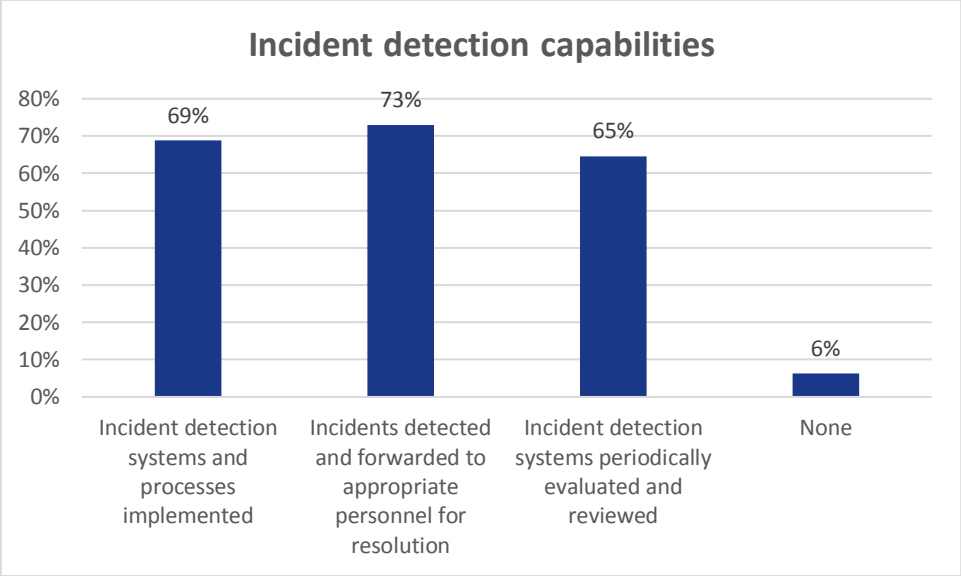


2.4.2 Incident detection capabilities

Almost 69% of providers have implemented incident detection systems and processes. For 73% of them incident detection is a continuous managed process that involves detection of incidents and their forwarding to appropriate personnel for resolution. About 65% of providers review their incident detection systems periodically while using network and information changes as well as past incidents to improve incident detection capabilities. The deployment of basic intrusion detection systems and process

implementation are slightly lower than expected given the high number of respondents indicating implementation of the incident management processes. It is likely to be attributed to the existence of written policies and procedures that are not necessarily supported by operational capabilities.

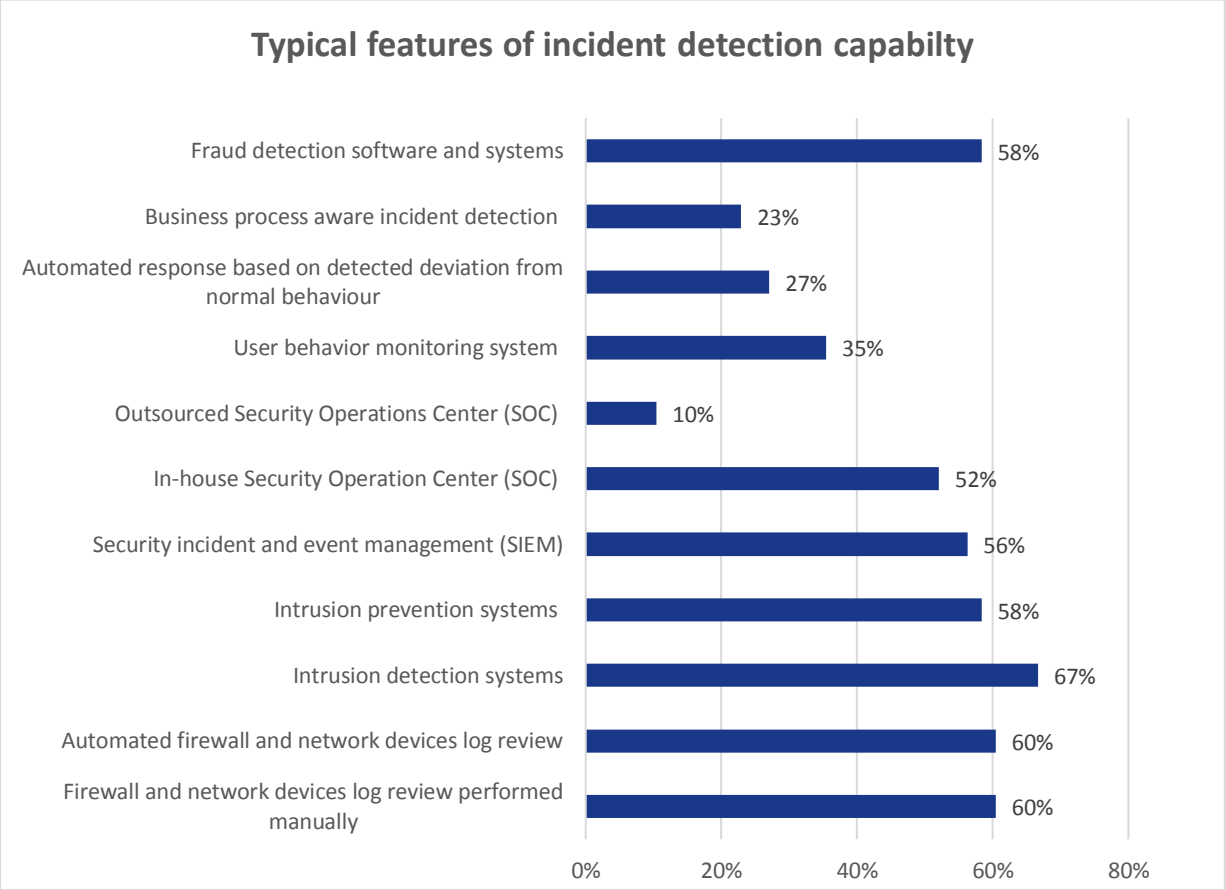
Figure 13: Level of incident detection capability implemented



Incident management records and reports are created for major incidents when considered relevant. Within the scope of Information Security, incident management is more mature for continuity-related incidents (more frequent) and less mature for personal data related incidents (less frequent).

Intrusion detection systems are the most widely used incident detection capabilities with two thirds of the providers stating they have them in place. 60% of providers do manual log review of firewall and network devices and the same number of providers have this process automated. In-house Security Operation Centre is the case for 56% of operators, while only 10% have this facility outsourced. User behaviour monitoring system is used by 58% of providers while around 23% of them have implemented business process aware incident detection, both of which can be considered as a very good achievement.

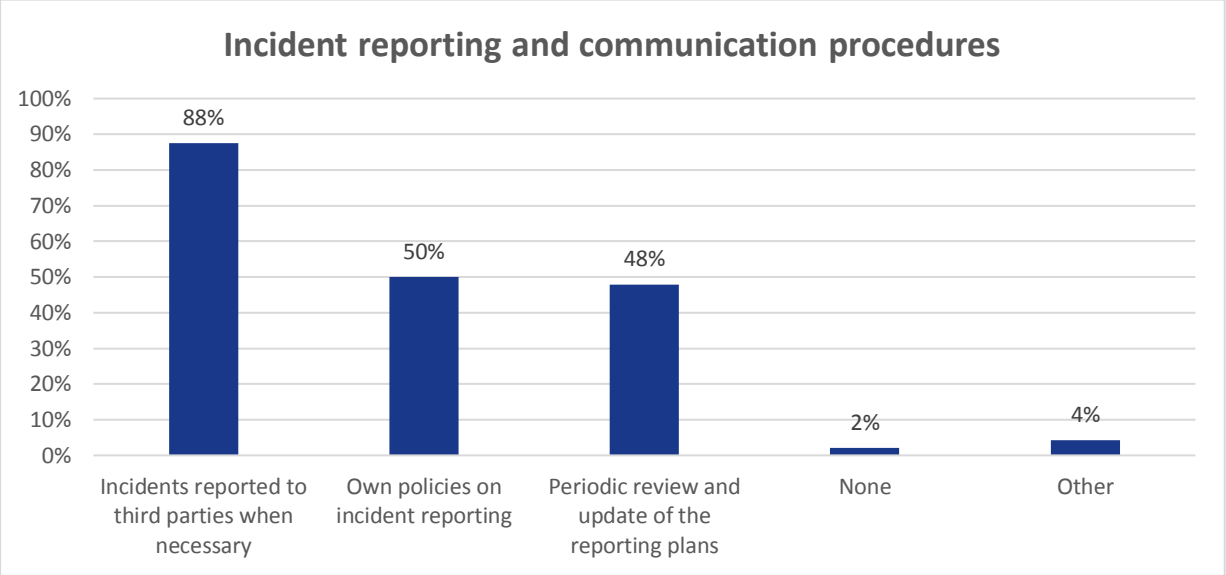
Figure 14: Typical features of incident detection capability



2.4.3 Incident reporting and communication procedures

The providers are recommended to establish and maintain sound procedures for incident reporting and communication that take into account national regulations on incident reporting to government authorities. A total of 87.5% of providers communicate and report incidents to third parties like government authorities and their customers. Only 50% of them have their own policies in place on incident reporting which includes reasons and motivation for communication, the incident type, reports' content, communication channels and communication roles, templates for incident reporting etc. Even lower number (48%) of providers carry out a regular review of the reporting and communication plans.

Figure 15: Incident reporting and communication procedures



Notification to NRAs and customers is usually carried out under the requirements of Article 13a, which were transposed to national legislation. The communication procedures are focused on service interruption incidents, which are related to impact on customers, services provided and the resulting reputation of the company.

2.5 Business continuity management

2.5.1 Disaster recovery capabilities

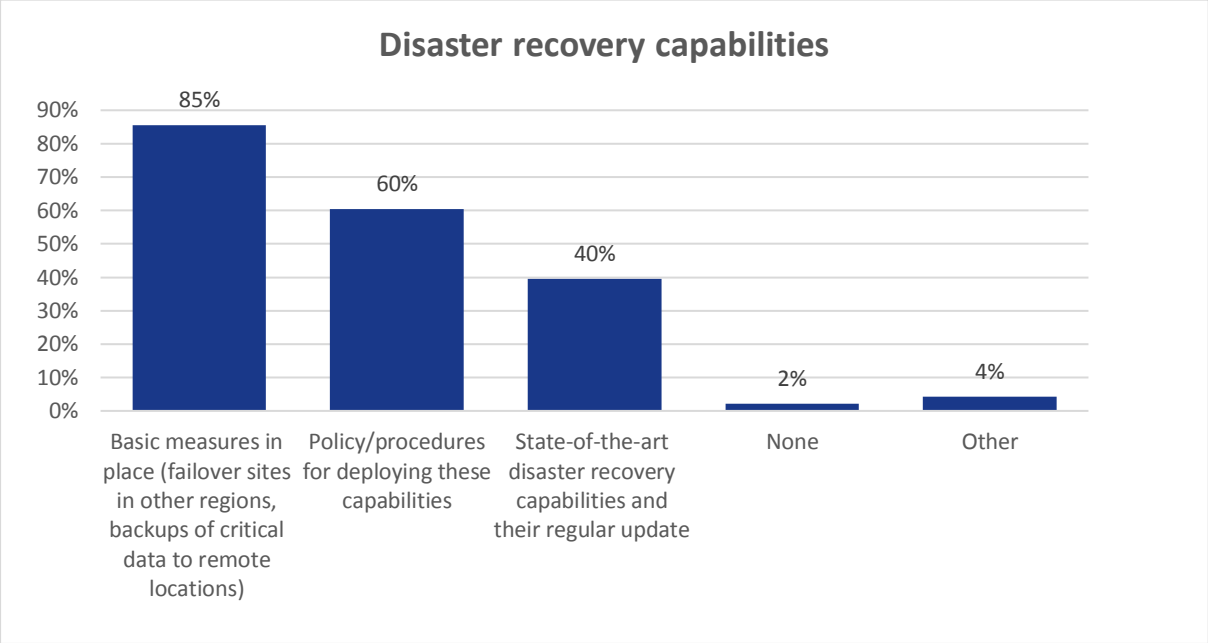
Disaster recovery capabilities serve to restore network and communication services following natural and other major disasters. More than 85% of providers have implemented basic measures in this regard as failover sites in other regions or backups of critical data in remote locations.

About 60% of surveyed providers have documented policies for deploying these capabilities, which may include list of disasters with a potential to impact upon service provision as well as a list of disaster recover capabilities available internally or provided by third parties.

Roughly 40% of providers have set up state of the art disaster recovery capabilities like full redundancy and failover mechanisms. They also review their disaster recovery capabilities regularly. All numbers indicate an overall high maturity of operators in disaster recovery capabilities.

One of the operators has provided valuable insights to their disaster recovery measures: *"In addition to DR for some services, the network architecture is defined to incorporate, when relevant, redundancy capabilities. For example, some network platforms are implemented in a balanced/distributed architecture (i.e., all the network traffic is distributed between all the identical platforms). In case of failure of one of those platforms, the traffic is automatically re-routed. This can be considered an Active-Active architecture, instead of the Active-Passive architecture of the DR."*

Figure 16: Disaster recovery capabilities



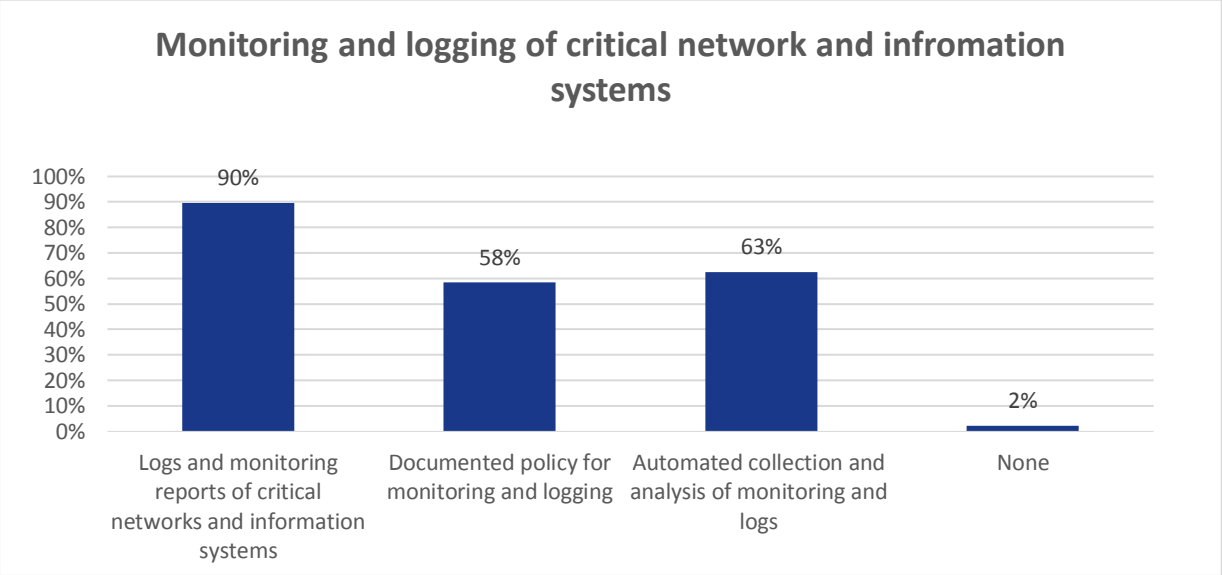
2.6 Monitoring, auditing and testing

2.6.1 Monitoring and logging of critical network and communication systems

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified. Around 90% of providers indicate that they carry out logs and monitoring reports of critical network and information systems.

A much lower number (58%) of providers have also implemented policies for monitoring and logging including minimum logging and monitoring requirements. A very high share 63% of operators have set up tools for automated collection and analysis of monitoring data and logs.

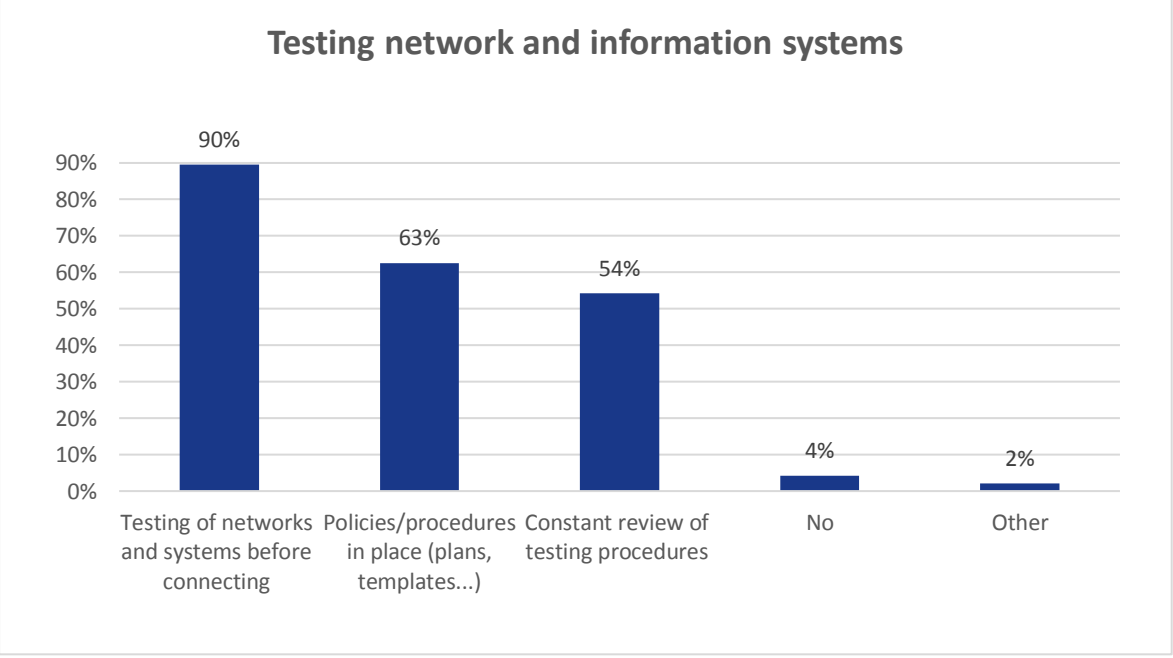
Figure 17: Monitoring and logging of critical network and information systems



2.6.2 Testing network and information systems

There should be policies in place for testing network and information systems, especially when connecting to new networks and systems. Rigorous testing of systems and network equipment saves a significant amount of time by reducing troubleshooting times and improves network availability. Just like with monitoring approximately nine out of ten providers produce test reports of the network and information systems, which includes tests following big changes or the introduction of new systems. A majority of 62,5% claim to have policies and procedures in place as well as tools for automated testing. 54% of them review and update testing policies and procedures.

Figure 18: Testing network and information systems

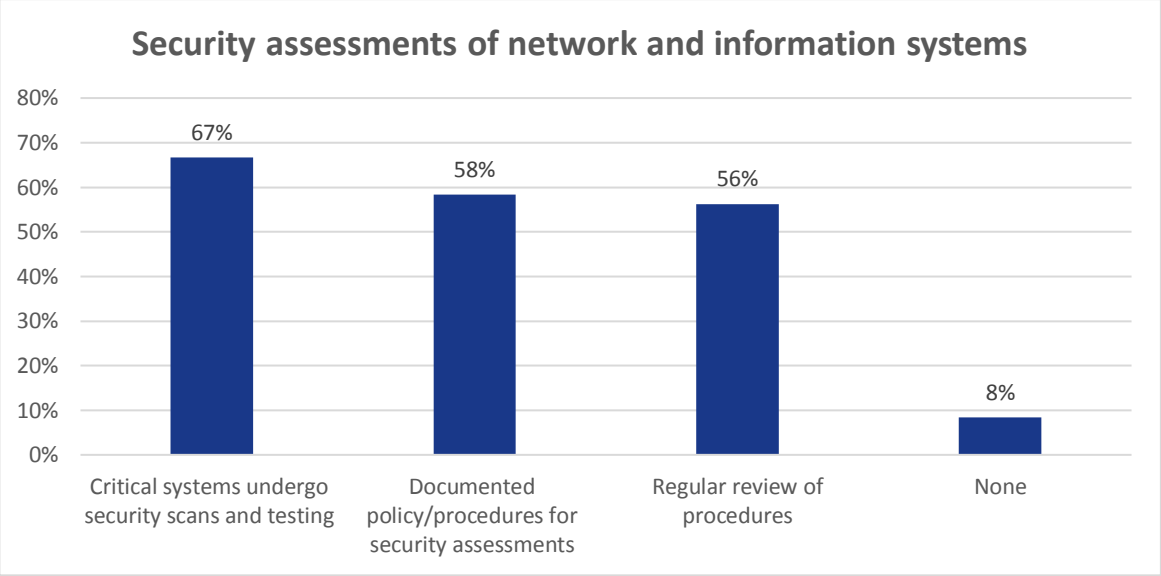


2.6.3 Security assessments of network and information systems

The providers should undertake security assessments of network and information systems. This covers, inter alia, also penetration testing and vulnerability assessments. The security assessment is a tool that ensures intended functionality of security controls. Only two thirds of operators carry out regular security scans and testing especially when introducing new systems or following changes. While it is possible to use an availability as an excuse this number can be improved by performing security assessments of sliding schedule or combined with failover testing.

A somewhat lower number (58%) of providers have in place documented procedures/policies concerning the types of assets, the circumstances, frequency, confidentiality levels for assessments and test results etc. as one of the surveyed providers put it: "We have policies for secure development of applications and services and secure infrastructure implementation that include security testing checklists and risk evaluation matrixes." Some 56% of providers undertake regular review and update of these procedures.

Figure 19: Security assessments of network and information systems

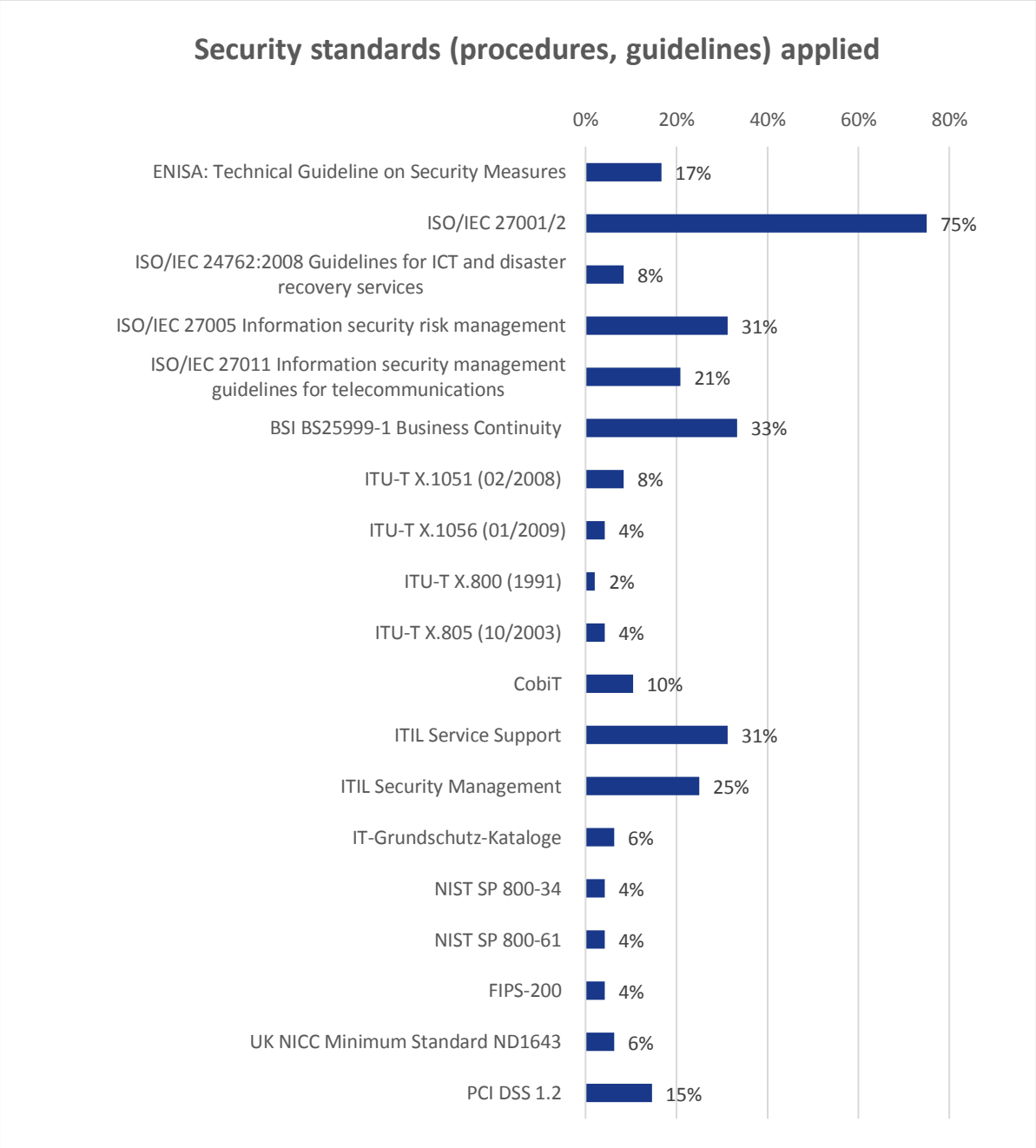


2.7 Security standards, frameworks and guidelines

The security measures used in ENISA documents have been often adapted from various existing international network and information security standards, guidelines and good practices. These standards, that may be either mandated or recommended to the providers, provide them with guidance, terminology, structure for supervision and auditing, baseline etc. Standards of ISO, especially ISO/IEC 27001 "Information security management systems" are the most widely used with 75% of providers claiming to adhere to the ISO 27001. On the positive side it is worth to mention the proliferation of standards and frameworks the practicality of which has been proven by the number of adopters in various industries, including those other than the electronic communication providers. ISO 27000 group of standards and parts of ITIL Service Management Framework have been reported with the highest adoption rate. ENISA's Technical Guideline is used by 17% providers. It was designed rather as a "soft approach" guideline only and is probably seen as a driver for adoption of more detailed and more specific frameworks and standards. It is also surprising to see such a high level of providers indicating the adoption of ISO 27001 standard, that contains Information Security Management System (ISMS) performance evaluation and

improvement requirements, while a significantly lower number in reality carries out periodic review of efficiency of various security controls. This discrepancy suggests that even reported standards and frameworks

Figure 20: Security standards, frameworks and guidelines used by European providers



2.8 Measures against DDoS attacks

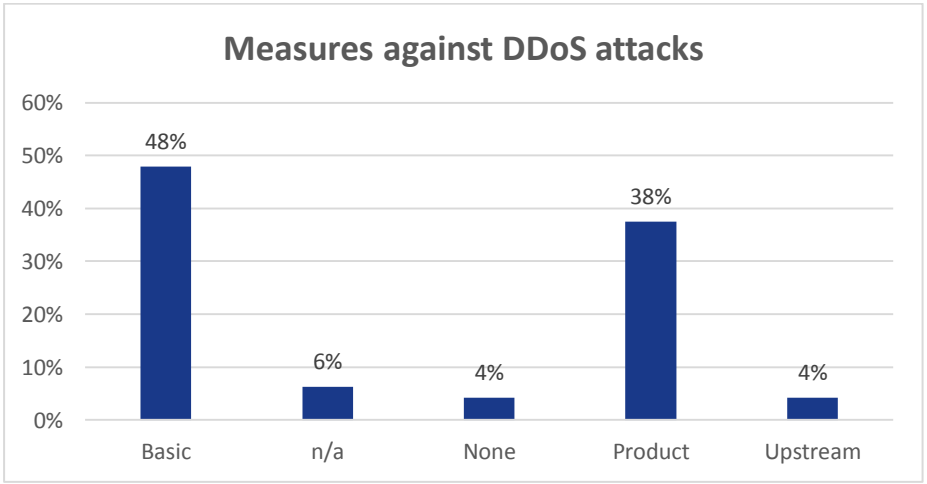
Distributed Denial of Service (DDoS) is a type of denial of service attack where multiple compromised and/or infected systems target a single system causing it to fail due to traffic/requests overload. There are many types of DDoS attacks, for example:

- Transport protocol based attacks aim to overload the target system with large volume of TCP, UDP, or ICMP requests forcing the loss of similar requests from legitimate sources thus rendering the target system non-responsive.
- Bandwidth exhaustion attack is similar to the above with the difference that malicious agents try to overload the target with large amounts of bogus data.
- Application level attacks exploit application limitation to process requests in volumes and sizes generated by malicious agents. While specific application may be under DDoS attack, other applications running on the same infrastructure may also be affected as application competes for computational and memory resources in an attempt to handle the requests volume.

Slightly more than a half of the providers indicate use of configurations (traffic limitation) to counter DDoS attacks as well as close monitoring. Approximately a half of them use specialized hardware (i.e. Arbor Networks) and less than 10% rely on upstream providers for DDoS mitigation. According to ENISA Annual Incident Report for 2015 the incidents caused by malicious actions (e.g. DDoS), although there were not many of them, had most impact in terms of duration, which lasted on average almost two days per incident.[13]

Based on the low percentage of incidents the conclusion is that the defenses employed by providers are sufficiently effective. At the time of writing, however, DDoS attacks had been on the rise with the use of Internet of Things (IoT) devices as malicious agents.[14] Those attacks are characterized by a significantly increased volume of traffic so deployed defenses should be evaluated for the capability to withstand the new attack levels.

Figure 21: Measures against DDoS attacks



[13] https://www.enisa.europa.eu/publications/annual-incident-reports-2015
[14] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/

2.9 Measures for the SS7 protocol

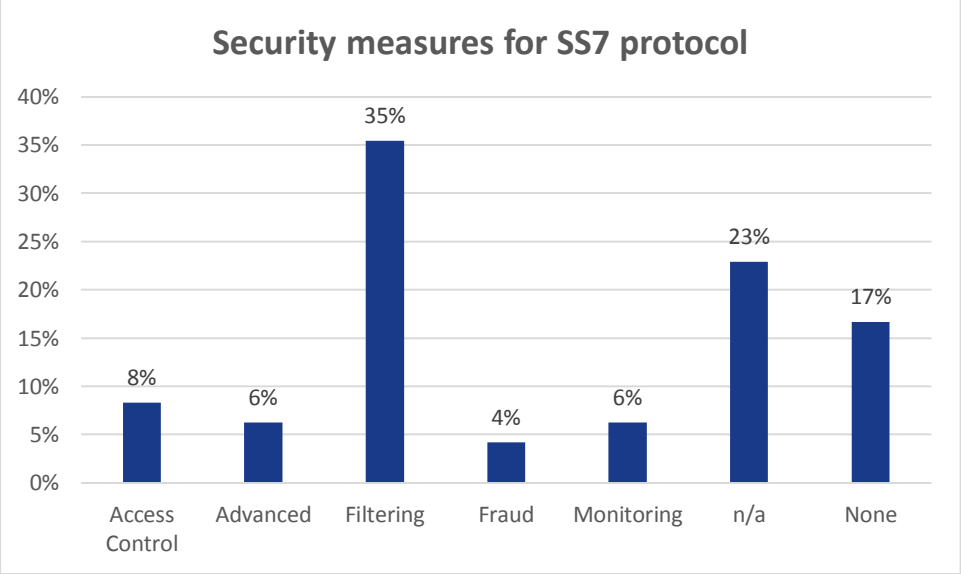
SS7 protocol based attacks present a significant threat not only to the service providers but also to the users to the point where the attacker can not only track the user location and access the information on the connected mobile device, but also redirect the calls.[15] [16] [17] Security measures are required to protect attackers from:

1) Accessing private data residing on user's mobile device;
2) Committing fraud e.g. transfer of funds;
3) Disrupt normal operation of the network.

Due to the age of the SS7 protocol (it was designed in the 70s) the majority of the security issues lie in the architecture and configuration design and are not easy to resolve.

SS7 protection is a topic with a high diversity of security measures implemented. About 40% of respondents indicated deployment of the SS7 firewalls with additional less than 10% relying on access controls to prevent unauthorized access to the SS7 network. The rest of answers range from monitoring, SS7 intrusion and fraud detection systems to administrative/procedural controls. As no data is available to determine the widespread occurrence of SS7 specific security incidents it is difficult to reach a conclusion on the subject given the variety of methods employed.

Figure 22: Measures for SS7 protocol



[15] SS7 hack explained: what can you do about it? https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls
[16] SS7 Attack Circumvents WhatsApp and Telegram Encryption - May 10, 2016 http://news.softpedia.com/news/ss7-attack-leaves-whatsapp-and-telegram-encryption-useless-503894.shtml
[17] ITU Workshop on "SS7 Security" http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx

3. Key points and Recommedations

All-in-all, approximately 60% of providers report a very good level of compliance with ENISA security requirements, while virtually all providers have deployed a good level of basic security controls. In some security domains, the level of maturity reported is high as well as the sophistication of implemented controls. Security of systems and facilities is an example of a security domain with a relatively high maturity of measures adopted. For other domains, though, there is an ample room for improvement, in particular as regards the availability of specific policies and operational documentation is lower than desired.

With a growing sophistication of attacks the basic level of security controls may not provide sufficient protection and the higher level of security controls maturity is essential. Many providers seem to realize the necessity of qualitative security control improvement and have deployed sophisticated technical controls. A key conclusion seems to be that while all IT security basics are covered, the achievement of the next level of maturity is impeded mostly by lack of sustainability mechanisms, i.e. repeatable processes and the regularly maintained documentation.

A general quantitative breakdown based on self-assessment indicates that approximately 25% of providers have advanced capabilities in one or more security domains, and approximately 60% have satisfactory capabilities in all domains. Below are the quick conclusions drawn per each security domain. A three-grade maturity scale is applied for the conclusions on individual security domains.

Satisfactory	High	Very High
Providers indicated presence and functionality of basic security controls.	Providers indicated presence of advanced security controls and ad-hoc processes in place, usually in reaction to a security event.	Providers indicated proactive security posture with combination of advanced and basic security controls verified regularly according to well established policies and processes.

The main recommendation for the providers based on the analysis of the deployment of their security measures is to pay additional attention to the sustainability and efficiency. This is best achieved by the adoption of Service Management frameworks and by creating a system that includes measurement and periodic reviews of security controls and capabilities in all domains.

Governance and risk management

Domain Maturity level:

[Satisfactory]	High	Very High

Around 60% of respondents report good practices for security governance and risk management. The maturity level of the whole domain is ranked as satisfactory because high-level governance documents and their periodic review is a relatively low effort exercise. Therefore; it is expected that at least the basic level of maturity is reported by at least 90% of respondents. Only 56% of providers employ the risk management methodology, while registering the risks is a first step towards effective risk management

program and is reported by 65% of providers. It is surprising that there is not a higher number of providers taking the next step of addressing risks with mitigation techniques.

Domain recommendations:

- Improve governance by utilizing templates provided as references in the section **Error! Reference ource not found.** to develop necessary company-wide topics for all aspects of security.
- The starting point for proper risk management should be ISO 27005[18] standard to turn risk management from ad-hoc human-driven activity into the properly managed business process.
- Select and adopt ISO or any other risk management framework that allows to build the processes to regularly and systematically address risks registered in the lists of risks.

Security of systems and facilities

Domain Maturity level:

Satisfactory	**[High]**	Very High

High level of implementation of soft- and hardware based tokens for multi-factor authentication as well as a significant presence of biometric authentication would make security of systems and facilities one of the domains that demonstrates a very high maturity. Unfortunately, this significant achievement is offset by only a very basic set of integrity controls. Preventing unauthorized changes to the systems is as important as proper access control. Undesired changes are not necessarily a consequence of an attack, but often a result of a simple human error. The detection of the binary or configuration file modification by integrity controls provides an additional layer of system security. In this respect it is noteworthy that some of the eCommunication providers have realized the significance and deployed system-level file integrity controls on critical systems and even built capability to automatically restore system to desired state in the case the said state has been altered.

Domain recommendations:

- Improve integrity controls by a wider adoption of file and filesystem-level integrity controls.
- Pay a particular attention to automated restore of desired configuration for critical systems and integrity control of binary and configuration files deployed on them.

Operation management

Domain Maturity level:

[Satisfactory]	High	Very High

The operation management domain is a perfect illustration to the overall conclusion summarized at the beginning of this chapter. 81% of providers follow predefined procedures for change management and 90% have the responsibilities assigned. With all basics covered the number of respondents who document

[18] http://www.iso.org/iso/catalogue_detail?csnumber=56742

their change management procedures falls to 65%, and even further when it comes to a periodic review of change management procedures – this is done by only 56% of respondents. This is aligned with another data point – low percentage of respondents who are utilizing ITIL framework. Service management frameworks allow for a better service delivery that in turn leads to higher customer satisfaction and reduced incident costs.

Domain recommendations:

- Adopt Service Management framework (e.g. ITIL) in particular where it describes change management.
- Keep in mind that change management process is tightly connected to both problem and incident management.
- Document de-facto processes, nominate process owners with assigned responsibility for periodic review and update of operation management documentation.

Incident Management

Domain Maturity level:

[Satisfactory]	High	Very High

This domain too that has well developed detection capabilities that are followed by incidents being assigned to appropriate personnel for resolution. However, when confronted with a list of specific controls that are part of their incident management capability, the providers emphasize the detection capability while review and update of procedures lack behind. The same value around 60% is reported for everything from fraud detection capabilities to automated log reviews. It is interesting to see that half of respondents run in-house Security Operation Centers, but 60% indicate that they review the logs manually with only 56% having Security Information and Events Management (SIEM) systems deployed. Process-based incident detection is reported in only 23%. On the positive side it is necessary to mention that slightly above a quarter of respondents (27%) indicated that they are using automated response based on detected deviation from normal behavior and 35% have user behavior monitoring. Therefore the same conclusion as before: The majority of eCommunication providers have stopped at basics of incident management with less than half (48%) reviewing and updating their incident reporting plans.

Domain recommendations:

- Adopt Service Management framework (e.g. ITIL) in particular where incident response procedure is connected to root-cause analysis activities and subsequent problem management process.
- Analyze de-facto as well as documented processes for the possibility of introducing high-level incident detection controls, define incident response trigger points at process level.
- Assign process-based incident detection controls review to the process owner.

Business continuity management

Domain Maturity level:

Satisfactory	**[High]**	Very High

High maturity domain together with Security of Systems and Facilities with 40% stating they have state-of-art disaster recovery capabilities and regularly update them. A significant number of providers (85%) indicate availability of remote backups and geographically dispersed fail over sites.

Domain recommendations:

- Introduce regular testing and update of policies and procedures as part of semi-annual business continuity testing.

Monitoring, auditing and testing

Domain Maturity level:

Satisfactory	**[High]**	Very High

Another high maturity domain with a majority of respondents (90%) monitoring and testing critical system and networks. Standard 60% have policies in place for both monitoring and testing. Main room for improvement is security scan that lags below pre-deployment tests while it should be an integral part of testing procedure.

Domain recommendations:

- Make security testing part of pre-deployment testing procedure. Connect pre-deployment security testing with integrity controls, introduce integrity monitoring of the systems and networks.
- Reduce manual log analysis efforts by employing automated log review capabilities and integrate this capability with SIEM systems.
- Pay a particular attention to the effectiveness of automated capabilities (scanning and log review) to ensure the capability is aligned with current business requirements as is capable to address the ever changing threat landscape.
- Consider the adoption of Continual Service Improvement (CSI) if adopting the whole ITIL framework is not a business viable option.

Annex A: List of Security Domains and Objectives

SECURITY DOMAIN	SECURITY OBJECTIVES
D1: Governance and risk management	SO1: Information security policy SO2: Governance and risk management SO3: Security roles and responsibilities SO4: Security of third party access
D2: Human resources security	SO5: Background checks SO6: Security knowledge and training SO7: Personnel changes SO8: Handling violations
D3: Security of systems and facilities	SO9: Physical and environmental security SO10: Security of supplies SO11: Access control to network and information systems SO12: Integrity of network and information systems
D4: Operation management	SO13: Operational procedures SO14: Change management SO15: Asset management
D5: Incident Management	SO16: Incident management procedures SO17: Incident detection capability SO18: Incident reporting and communication
D6: Business continuity management	SO19: Service continuity strategy and plans SO20: Disaster recovery capabilities
D7: Monitoring, auditing and testing	SO21: Monitoring and logging policies SO22: Exercise contingency plans SO23: Network and information systems testing SO24: Security assessments SO 25: Compliance monitoring

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-07-16-153-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-205-9
DOI: 10.2824/074677