09-06-2020

# Deliverable D8.1
# Summary of Security Training and Awareness Campaign Materials: An Investigation and Gap Analysis of Current Security Training and Awareness Resources

**Deliverable D8.1**

| | |
|---|---|
| Contractual Date: | 31-12-2019 |
| Actual Date: | 09-06-2020 |
| Grant Agreement No.: | 856726 |
| Work Package | WP8 |
| Task Item: | Task 1 |
| Nature of Deliverable: | R (Report) |
| Dissemination Level: | PU (Public) |
| Lead Partner: | LITNET |
| Document ID: | GN4-2-19-338D84 |
| Authors: | Sarunas Grigaliunas, Klaus Möller, Stefan Kelm, Albert Hankel, Sigita Jurkynaite |


The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

**Abstract**
This document summarises which security training and awareness campaign materials are available to NRENs, and identifies areas where gaps exist and it would be beneficial to the GÉANT community to develop additional security trainings and materials, and explore new training approaches.

# Table of Contents

# Table of Figures



# Table of Tables

# Executive Summary

In view of the increasing importance of cyber security, WP8 Task 1 conducted two gap analysis to understand where it would be beneficial to the GÉANT community to develop additional security trainings and materials and explore new training approaches.

The first gap analysis focused on cyber security trainings and materials, finding that:

- NRENs expressed a need for more trainings on social engineering, spam, phishing, device security and strong passwords both internally and externally.
- Only 6% of the cyber security courses in the current training overview are in the category of Privacy Protection / Data Leakage Prevention. The majority of NRENS expressed a need to provide more training on GDPR and data protection topics.
- Only 3% of the trainings deal with Operational Network Security. NRENs would like to have more of this type of trainings, both at general and advanced levels.
- The number of cyber security trainings for management are insufficient. There is a need for more courses for the managers, boards and other governing bodies of both the NRENs and their member institutions.
- NRENs expressed the need for innovative training methods, such as gamification.

The second gap analysis concentrated on cyber security awareness campaigns and materials, finding that:

- While technical subjects of security awareness are well covered, more focus should be put on non-technical staff and management. Psychological and sociological aspects of cyber security should also be considered when designing awareness activities.
- Universities and other NREN member organisations have different needs, making it difficult for the NRENs to deliver unified security awareness services. However, it is important that topics related to data and privacy protection are addressed.
- NRENs would like GÉANT to take an active role in developing and leading more security awareness activities. These activities should be long-term, regular and include games, drills, films, etc.
- There is a need for Train the Trainer type activities to allow NRENs to run their own security awareness campaigns and joint events with all NRENs to promote their cyber security awareness.

Based on these findings, WP8 Task 1 will prepare recommendations and plans for the future activities that will address the needs of the NRENs and assist them in securing their networks and organisations.

# 1 Introduction

Cybersecurity is critical to European economies, the very functioning of democracy, and European values. Malicious cyber activities, in particular disinformation campaigns, fake news and cyber operations targeted at critical infrastructure and varying in scope, scale, duration, intensity, complexity, sophistication and impact, are becoming increasingly common. They demand a mobilisation of the full range of security tools and instruments, and a joint European response [Cybersecurity]. The definition of critical infrastructure varies by country, and for some it includes their National Research and Education Network (NREN). In the countries where an NREN is not included, the network is part of the essential communications and education sectors, where cyber protection is of undeniable importance.

Just like other organisations, NRENs are suffering from ever-evolving attacks. While having the right technologies is very important to protect an organisation from those and other threats, the vast majority of the incidents can be linked to a human error. Understanding that people are often the biggest threat to the security of sensitive information, users of information systems must be made aware of the cyber security risks associated with their activities. In addition, those with significant cyber security responsibilities must be adequately trained to carry out their assigned security-related duties. NREN community members are the first line of defence against contemporary security threats. Therefore, security training is one of the most important aspects of an NREN's security posture.

One of the goals of GN4-3 WP8 Task 1 *Business Continuity Recommendations* is to help NRENs with their security awareness and training efforts. Although NRENs' core activities and mission might be similar, the organisations themselves and their constituencies are very diverse, as is their level of cyber security preparedness. Taking those differences into consideration, Section 2 of this report identifies the security trainings and training materials that are available to NRENs, and details gaps where further material could be developed. Section 3 details existing campaigns and materials for promoting cyber security awareness, highlighting gaps where more security awareness is needed. Section 4 summarises the findings and offers a conclusion on the next steps forward.

# 2 Cyber Security Training and Training Materials for NRENs

Building cyber resilience and keeping organisations' day-to-day operations free from malicious interferences requires skilled staff members with both technical and operational skills. Cyber security is becoming an integral part of the training portfolios of NRENs when it comes to both the NREN staff, and the trainings offered to their constituents.

However, the need for improvement in this area was explicitly expressed by NRENs during the preparations for the GN4-3 project. In order to better understand what these requirements are and aid in the future planning of cyber security trainings within the GÉANT community, it was necessary to first gain an overview of existing trainings and of NRENs' specific needs. To this end, a two-pronged approach was followed:

1. Obtain a list of training courses in use through desktop research.
2. Examine the needs of NRENs through interviews with staff members of representative organisations.

These findings will be used to analyse the gap between the available trainings and the NRENs' requirements, in order to make recommendations and plan the future activities of WP8 Task 1.

## 2.1 Existing Training and Materials

During the first year of the project, the Task 1 team conducted research into which existing training programmes and materials could be used by GÉANT members. The team carried out extensive desk research, summarised the results, and added them to a list of trainings and training materials. The full table of these findings is given in Appendix A, and includes information on:

- the organiser of the training
- where to find the relevant information
- whether the training is available online
- whether a certification can be obtained
- the target audience
- the current known uptake by NRENs

The table consists of 76 entries and provided a good foundation for the research. However, it should be noted that this table intended to be a living document and will be continuously updated so that it can be used by the GÉANT community as a security training guide [Wiki].

The available trainings and training materials were grouped into 10 broad categories, allowing them to later be matched to the needs of the NRENs and identify any gaps. The ENISA Trainings Taxonomy [ENISA] was used as a starting point (categories 1 - 4 and 10). Categories 5 - 9 were added to reflect the different audiences (specifically for Research and Education (R&E), as the ENISA taxonomy was written for the study of information security training needs in critical sectors. Most of the categories in the taxonomy developed for this research cover security operations. The areas of risk management and general cyber security are covered under category 10 (General Cyber Security).

| | Training Category | Description |
|---|---|---|
| 1 | Cyber Security Foundations | Basic cyber security trainings, such as threat landscape, authentication issues, malware types, cryptography, and network security. |
| 2 | Audit / Penetration Testing / Ethical Hacking | Trainings related to security audits, penetration testing, and ethical hacking. |
| 3 | Monitoring | Trainings related to Network Monitoring, Intrusion Prevention & Detection systems (IPS/IDS) and Security Information & Event Management (SIEM). |
| 4 | CSIRTs/Incident Response | Trainings related to Computer Security Incident Response Teams (CSIRT) or Security Operation Center (SOC) activity, incident handling, and management. |
| 5 | Forensics | Trainings related to forensics. |
| 6 | Privacy Protection / Data Leakage Prevention | Trainings related to Privacy Protection (including GDPR), Data Safety, and Data Leakage Prevention. |
| 7 | Operational Network Security | Trainings related to network security for network operators, Routing Security, DNS Security, and DDoS protection. |
| 8 | Cloud Security | Trainings related to securing cloud infrastructures. |
| 9 | Secure Coding/ Vulnerability Management | Trainings related to Secure Coding, Secure Software Development Lifecycle (SDL) and Vulnerability Management. |
| 10 | General Cyber Security | Other security trainings, which are not particularly connected to the specific areas of cyber security covered above. |

Table 2.1: Cyber Security Training categories for R&E

To gain a picture of which areas of cyber security are most covered by the courses and training materials currently available to NRENs, each of the available trainings and materials on the compiled list (see Appendix 1) was assessed and assigned a number based on the defined categories (1-10). The courses and materials in each category were then counted to give an overview of current coverage.

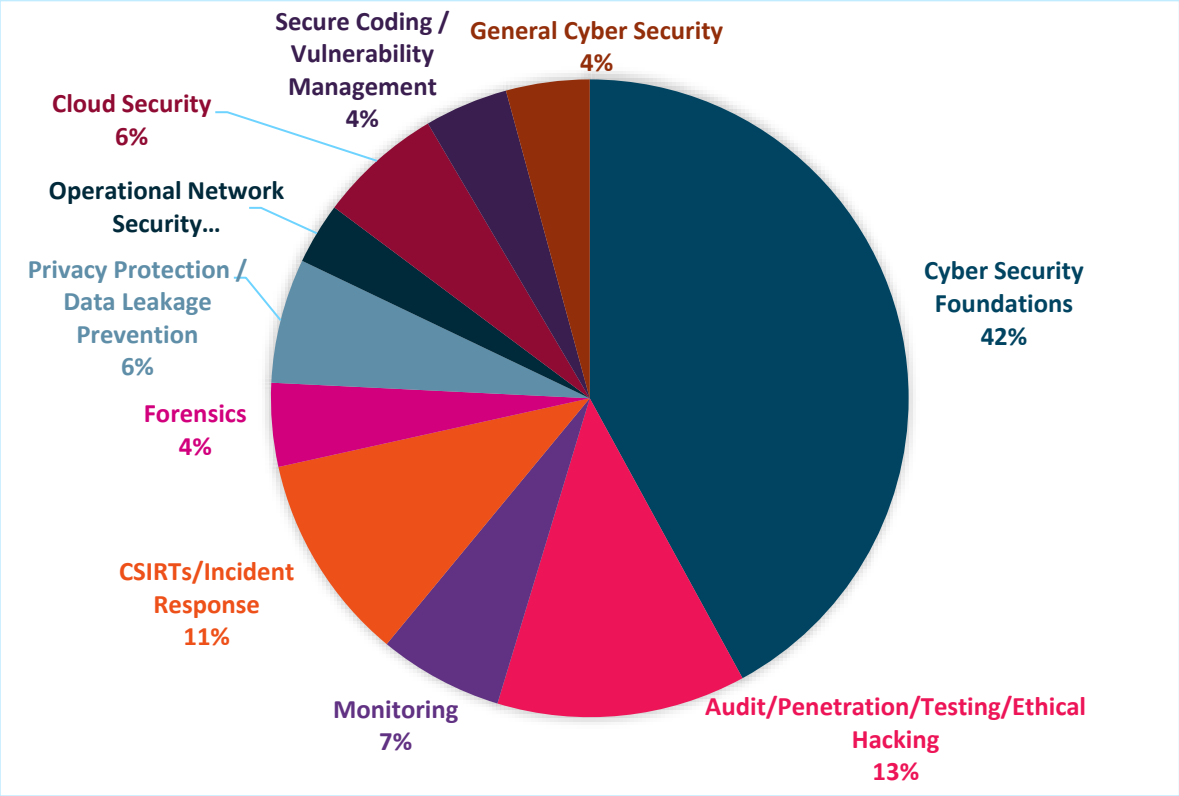


Figure 2.1: Cyber security training content category coverage

Most of the trainings and materials cover the topics in the Cyber Security Foundations (1) category. The next most covered categories are Audit / Penetration Testing / Ethical Hacking (2) and CSIRTs/Incident Response (4). Operational Network Security (7) is the least covered category.

To better understand the accessibility and impact of the courses that are currently available, NREN staff and members of the NREN constituency were put into three primary groups depending on their roles:

- Management (at different levels of organisations/infrastructure)
- Technical staff (responsible for parts of the infrastructure and/or services it provides, including system- and network-administrators, operators and IT-security personnel)
- Users (people who use the infrastructure to conduct their work, typically not security experts; non-technical staff, students, pupils, etc.)

The Management and Technical groups can be subdivided further as follows, to reflect the NREN and their members' situation better:

| Group | Sub-Group | Description |
|---|---|---|
| Managers | Technical | People in management positions/roles that have a strong technical background in IT. |
| | Non-technical | All other people in management positions. |
| Technical | Developer | Technical personnel whose main role is that of IT developers, architects, or designers. |
| | Security | Technical personnel whose main role is that of CSIRT members, security auditors, or security administrators. |
| | Admin | Technical personnel whose main role is that of administrators or operators not listed in the above roles. |
| Users | Non-technical | People who use the infrastructure to conduct their work, typically not security experts; non-technical staff, students, pupils, etc. |

Table 2.2: Sub-divided groups by role

All the trainings on the list of currently available cyber security courses and materials (see Appendix A) were assigned a target audience group based on their content. Three quarters of these are targeted at technical personnel, and for the most part consist of general security trainings for technical staff or courses for security personnel. There are two courses that are targeted specifically at Technical Managers and two for management generally, both technical and non-technical. No cyber security trainings are available specifically for non-technical management. The list includes five courses targeted at end users, while another 10 are interdisciplinary cross-category trainings aimed at various target audiences.

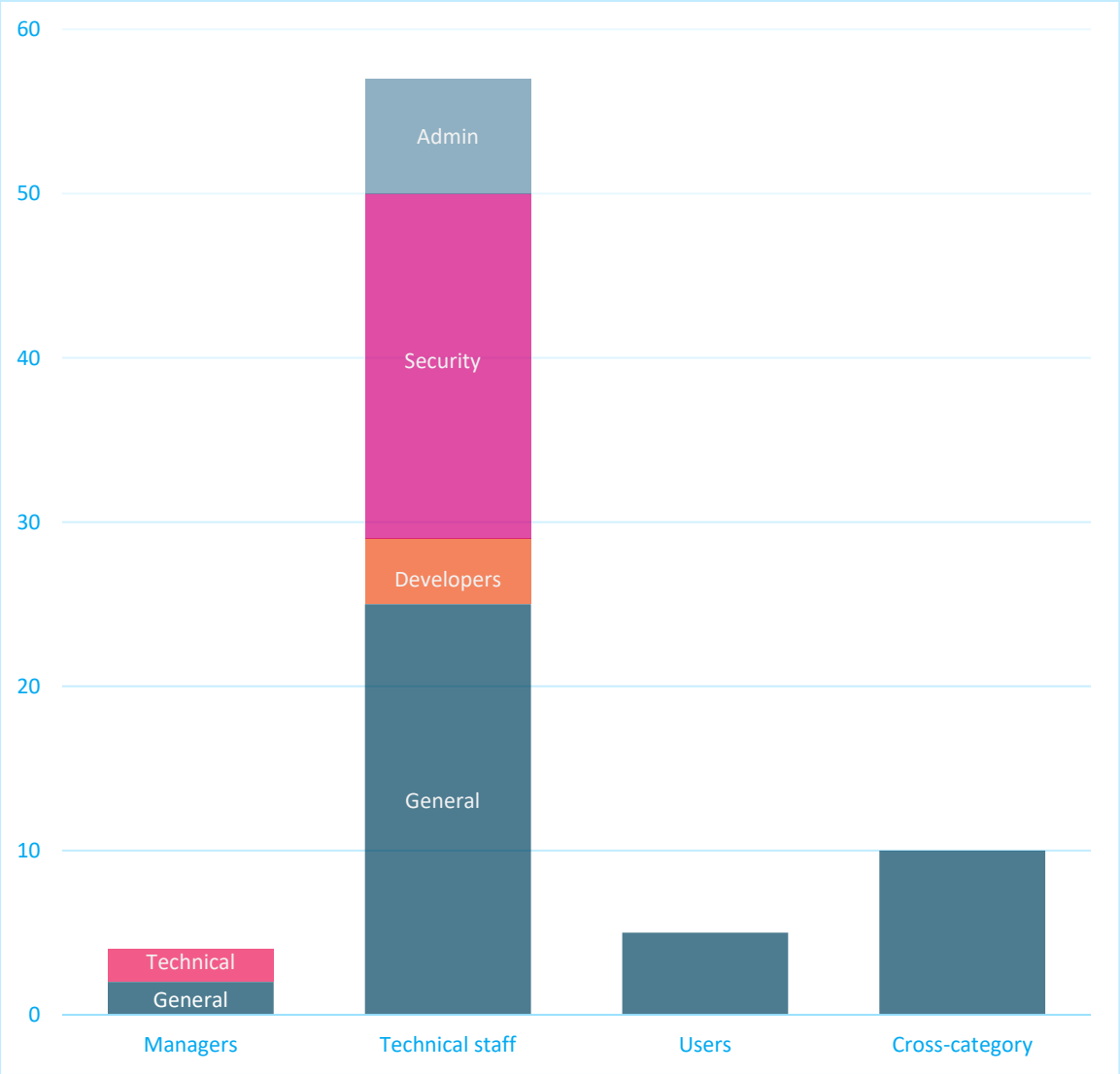


Figure 2.2: Cyber Security trainings per target audience

## 2.2 Interview Results

The second stage of the research into the current cyber security training availability for NRENs involved conducting interviews with members of 15 different NRENs across Europe to gain a deeper insight into their situations and needs. The NRENs interviewed were diverse in terms of geography, size, number of staff and membership, selected to be representative of the GÉANT community.

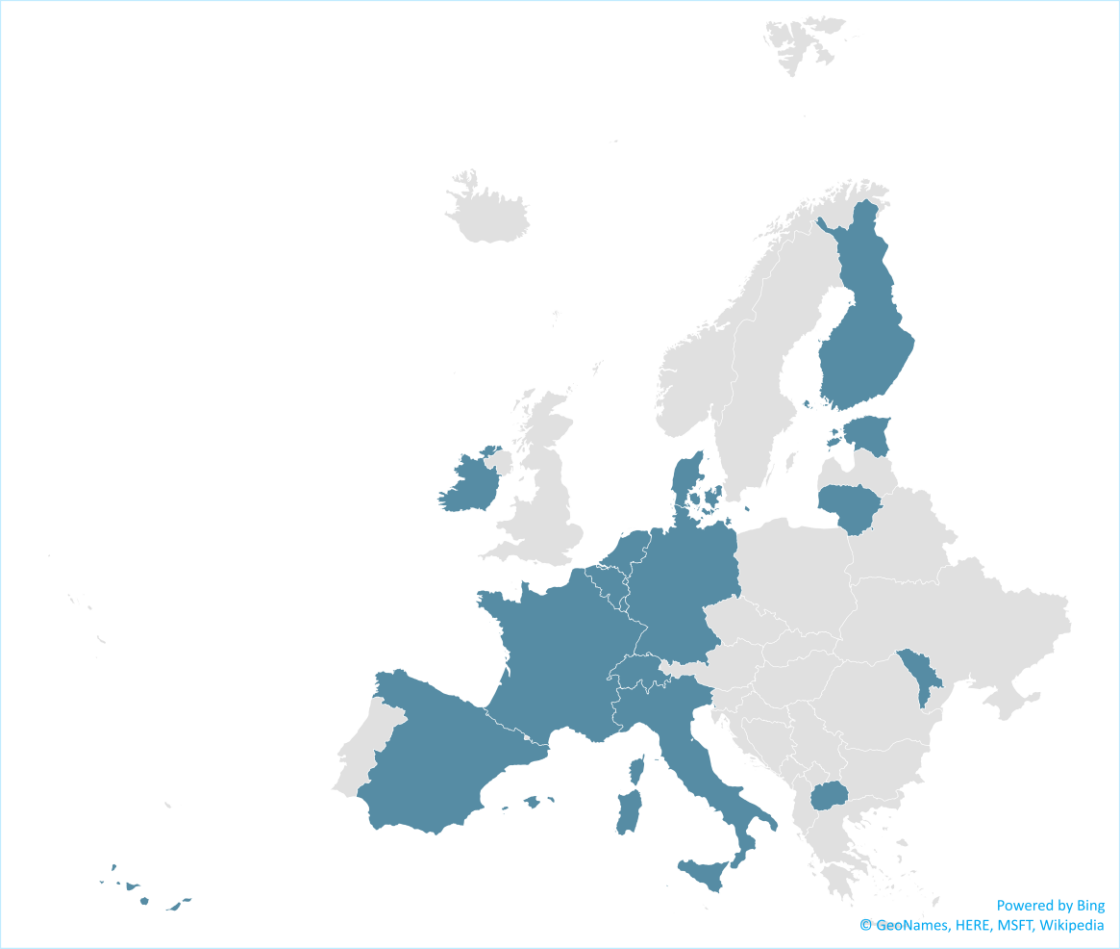


Figure 2.3: Map of interviewed NRENs

The interview questions covered three areas:

- General questions about the NRENs' cyber security training programmes.
- Information about the topics covered by the training programmes, both internally for the NREN staff and externally, by and for their member organisations and their constituencies.
- Information about the target audiences covered by the training programmes, both internally for their own staff as well as externally for their member organisations.

### 2.2.1 General Questions

Of the interviewed NRENs, two-thirds stated that they provide some cyber security training internally to their personnel and a little over half to their members externally. TRANSITS (CSIRT personnel training, coordinated by GÉANT) was mentioned most often, followed by the courses offered by ENISA and FIRST. The majority of the NRENs stated, however, that they did not have a comprehensive, formal programme. In many cases, the training courses offered were described as 'home grown' and 'demand driven'. The ways in which the training courses are provided include a variety of in-house workshops, trainings at conferences, and training courses from experts, depending on the individual NREN.

When asked for their reasons for not providing cyber security training as part of their internal and external training offering, the majority of the NRENs (60%) stated this was due to a lack of funds. Others mentioned insufficient priority and resources. 20% stated that they had not (yet) found suitable materials. When it comes specifically to trainings for their member institutions, the majority (over 70%) of NRENs stated that their members did not express a need for cyber security trainings.

### 2.2.2 Topic Coverage

The training courses run **internally** by the NRENs mainly fall into three categories:

- Cyber Security Foundations (covering topics such as password security, physical security, social engineering/phishing and detection and defence against spam)
- CSIRT/Incident Response
- IT Forensics (malware analysis)

The NRENs were also asked to describe their needs in terms of training their own staff. The majority of the topics mentioned in this area fell into the Cyber Security Foundations and Privacy Protection/ Data Leakage Prevention categories.

Table 2.3 below is a summary of the topics that the NRENs would like to have covered in security trainings for their staff but are currently not offering.

| Category | Topics |
|---|---|
| Cyber Security Foundations | Social engineering<br>Spam (detection and defence)<br>Phishing (detection and defence)<br>Laptop / Mobile Device Security<br>Password enhancements or replacements (i.e. 2-factor authentication) |
| Privacy Protection / Data Leakage Prevention | Privacy protection (GDPR)<br>Data classification, anonymisation<br>Data storage/safety<br>Data sharing in clouds<br>Data leakage prevention<br>Intellectual property (protection)<br>Privacy by design |
| Operational Network Security | General operational network security<br>Advanced network security<br>Setting up ‘walled garden environments’ (in WLANs)<br>BGP security |
| Cloud Security | Public/private clouds |
| Audit / Penetration Testing / Ethical Hacking | Penetration testing |

| Category | Topics |
|---|---|
| Forensics | Advanced network and software forensics |
| Other | Cyber security for non-technical personnel<br>Communication skills:<br>- communication between technical and non-technical personnel)<br>- cooperation of NREN technical staff (for experts)<br>Scenarios/artefacts for cyber exercises<br>Business continuity plan development |

Table 2.3: NREN needs for internal security training topic coverage

When asked asked about the topics covered by cyber security training provided **externally** to their member organisations, the majority of the interviewed NREN representatives responded that they either do not offer any such training to their members or were not able to answer because they did not have enough information about this.

In general, many of the NRENs interviewed indicated that offering such training is currently out of scope for them, and almost half of them could not answer what topics they would like to have covered if they were to offer it. Several of the NRENs mentioned a need for courses such as TRANSITS, trainings on DDoS mitigation and network security. Others raised the need for training on general information security (phishing, browsing, password management), business impact analysis and risk/crisis management.

### 2.2.3 Target Audience Groups

Asked about the target audience groups supported by their internal cyber security trainings, over half of the NRENs stated that they provide some kind of cyber security training to their technical staff, including cyber security staff/CERT, NOC, technical admins, IT team leaders and administrators. Over a quarter of the surveyed NRENs said that the trainings they offer are for all staff and anybody can sign up. Only two NRENs offer cyber security trainings for management.

Given the above, it is not surprising that the NREN management, board and governance, followed by non-technical personnel, were often mentioned as the groups that could be better supported.

Although the majority of the NRENs do not offer cyber security training for their member institutions, those that do so mainly provide it for technical/IT staff. If external training were to be offered, the surveyed NRENs would like to pay more attention to management, administrative staff, and non-technical staff, as well as, to some extent, to the end users (professors, students, pupils).

### 2.2.4 Other Training Needs Expressed

In addition to general questions, and questions about training topics and target audiences, the NRENs were asked to express other wishes, needs and suggestions for cyber security training. The answers demonstrated that there is not only a need for specific training topics, but also for different ways of

learning, such as games (for example, escape room exercises), online trainings and webinars, train the trainer events, short videos on security topics. The importance of a certificate of attendance or the ability to attend a series of recommended trainings or events and receive certification in the end was mentioned by several NRENs.

When asked about the role of GÉANT in cyber security trainings, the majority of the NRENs said that it should be actively developing training programmes for its members as well as pointing them to existing materials and opportunities.

## 2.3 Gap Analysis: Cyber Security Training and Training Materials

From the review of the existing materials and the NREN survey results, the following gaps in the NREN cyber security trainings emerge:

- Although the majority of the trainings found during the desk research are in the category of Cyber Security Foundations, the NRENs expressed the need for more trainings on social engineering, spam, phishing, device security and strong passwords both internally (NREN staff) and externally (NREN member organisations).
- Only 6% of the cyber security courses in the current training overview are in the category of Privacy Protection / Data Leakage Prevention, but the need to provide more training on GDPR and various data protection topics was expressed by the majority of the surveyed NRENs.
- There are even fewer (3%) trainings on Operational Network Security., The NRENs would like to have more of this type of trainings, both at general and advanced levels.
- More than half of the available trainings are aimed at technical personnel and most of the NRENs are offering training for their CSIRT/NOC/IT staff. However, the number of cyber security trainings for management are insufficient. There is a need for more courses for the managers, boards and other governing bodies of both the NRENs and their member institutions.
- The NRENs expressed the need for innovative training methods, such as gamification.

# 3 Cyber Security Awareness Campaigns and Materials for NRENs

Information and Communication Technologies (ICTs) are increasingly part of daily life and, as with other technologies, there are risks involved in using ICT. These risks cannot be mitigated with technological solutions alone - regular security awareness activities addressing the human element of the equation are needed to reduce the risks as well. Increasing dependency on ICT, increases the importance of security awareness, which is key to creating a security culture.

NRENs work with security awareness on two levels. First, it is their responsibility to make their staff aware of the security risks and regulations involved in the use of ICT infrastructure and services. In addition, they can deliver awareness services to their constituencies. Such services might entail organising a national awareness campaign or creating materials, i.e. a toolkit, for universities and schools so that they can run their own awareness programmes.

As the various NRENs have different levels of maturity, mandates and/or positions with respect to their countries, as well as different constituencies, it is difficult to compare their security awareness materials, given that they deliver different services based on their specific needs. This means that what one NREN perceives to be a gap, may not be considered such by another.

In view of these differences, the picture presented in this section may not be a complete one, however, it can provide a general overview of the awareness campaigns and materials that are used by NRENs or are available to them. The available campaigns and materials are described first; existing gaps are then identified, based on which recommendations have been drawn up.

## 3.1 Existing Campaigns and Materials

There are several online sources, both open-access and commercial, providing security awareness materials. The list provided below (Table 3.1) is not intended to be exhaustive but to give some examples of what is available. In general, organisations have the choice of using generic public materials, training and assigning their staff to create their own awareness programmes or looking for a commercial solution that covers several aspects of security awareness. In addition to those listed here, there are many national sources of these materials, often in local languages.

| Source | Materials provided | Content types |
|---|---|---|
| ENISA | The European Union Agency for Cybersecurity provides many materials on security, including on awareness topics. | Reports, awareness materials, trainings |
| Stop Think Connect | STOP. THINK. CONNECT is the global (US) online safety awareness campaign to help all digital citizens stay safer and more secure online. | Awareness content for end users (videos, tips, etc) as well as organisations to build their own campaign. |
| SANS | SANS offers security awareness training classes, training, materials and everything needed to educate Security Awareness specialists and every end user within organisations. | Mainly offers training aimed at specialists to organise awareness; publishes many reports and a number of free resources to use. |
| KnowBe4 | Well-known commercial solution: 'KnowBe4 is the world's most popular integrated platform for security awareness training combined with simulated phishing attacks.' | Commercial platform offering many aspects of security awareness. |
| LUCY Security | Another commercial solution: 'LUCY allows organisations to measure and improve the security awareness of employees and test the IT defences.' | Commercial platform offering many aspects of security awareness. |

Table 3.1: Sources providing security awareness materials.

## 3.2 Interview Results

To gain a better view of the security awareness campaigns and materials used by the NRENs, the second part of the survey described in the previous section covered awareness related subjects. The same 15 NRENs were interviewed for both parts of the survey (Figure 2.3).

### 3.2.1 General Questions

Most (2/3) of the surveyed NRENs run **an internal security awareness programme** for their own staff. They often run different activities throughout the year, ranging from workshops to phishing simulations. They use posters or flyers to draw attention to specific themes and sometimes distribute complimentary gifts, such as webcam covers. However, they expressed that they would like to expand their awareness programme.

A third of the surveyed NRENs **do not deliver** security awareness services to their constituents. The reasons they gave for this are lack of funds, or that their constituency did not specify a need for it.

Even where such needs exist, it is difficult for NRENs to meet them as they tend to be quite diverse between the various universities and other institutes. However, some of the NRENs have developed suitable solutions to overcome this challenge. For example, SURFnet delivers a toolkit with which their members can create their own awareness programme. One of the key principles of this toolkit is its flexibility, which allows universities and other institutes to adapt the materials to their own visual style and/or local situation.

When the NRENs were asked about the specific **external** awareness programmes that they deliver for their members, it emerged that these are also diverse. Some NRENs, such as Uninett, help run a national awareness campaign. Others, such as SURFnet, help their constituency to run their own local awareness campaign by delivering tools and guidelines for a successful programme. These tools include posters, videos, e-learnings, games, workshops, etc. Similarly, there are NRENs such as HEAnet and RedIRIS that deliver awareness and general cyber security training courses to the staff of their member organisations. Finally, some NRENs such as Jisc deliver specific services for members to simulate phishing campaigns.

### 3.2.2 Topic Coverage

NRENs were asked how well they covered several topics in their internal security awareness campaigns or as a security awareness service to their constituency. It is evident (Figure 3.1) that most of the topics are better covered internally than externally towards the NRENs' constituencies. However, it is important to note that where a topic is not well covered, it is possible that there may not be a need for the NREN to do so.

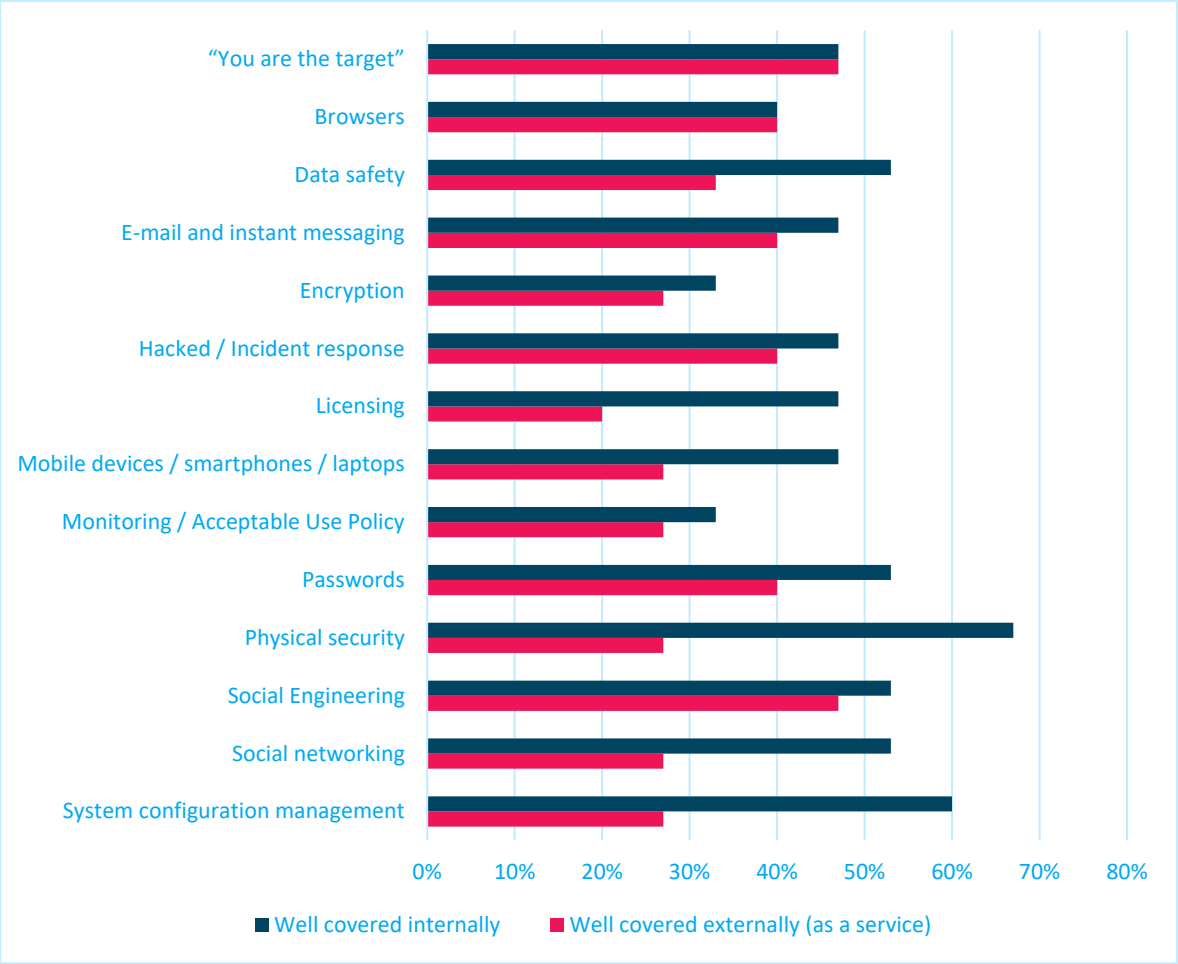


Figure 3.1: Security awareness topics covered by NRENs (% of NRENS that participated in the survey)

The best covered topics in NREN's internal security awareness campaigns are social engineering, social networking, passwords, data safety, physical security and system configuration management. Social engineering and 'You are the target' topics are best covered in activities aimed at the NREN member organisations and end users. The areas that need more attention are email and instant messaging (internally) and social networking and physical security (externally).

The NREN representatives were also asked about additional topics they would like to have covered by an internal cyber security awareness programme. Some of the suggestions were more general, for example relating to the importance of cyber security and the end user's role in it. Others listed more specific topics, such as sociological and psychological aspects of phishing and how to become more resilient to these attacks, handling of personal data in a resilient way and laptop security while travelling.

Additional topics mentioned for external awareness campaigns for the NRENs' members include intellectual property with regard to research data and privacy and data protection.

### 3.2.3 Target Audience Groups

A third of those NRENs that run an internal security awareness activity focus on all staff. Others run awareness campaigns for specific target groups, such as technical administrators, software developers and CSIRT staff. Some NRENs run awareness activities for non-technical staff, but only one runs an activity specifically for management. When asked which groups could be better supported, almost half of the NRENs indicated management as the single group that needs to be covered better.

When it comes to external awareness services for their constituents, the survey results show that the majority of the NRENs that provide such services are targeting students (63.6%). The second biggest target group are university staff (45.4%), followed by IT administrators (36.6%). Half of the NRENs would like to support their member organisations and their constituencies better through security awareness services, but no one particular group of end users stands out as target. The respondents mentioned professors, directors, students, non-IT staff, parents and system administrators as the potential target audiences.

### 3.2.4 Other Security Awareness Needs

Similar to the answers given to questions about training, when asked for additional comments about security awareness the respondents mentioned the need for innovative ways of raising awareness and running activities, such as games, drills, and short films that can be translated into other languages. The importance of the psychological aspect in increasing awareness was raised a few times, also with reference to dealing with feelings associated with cyber security (frustration, powerlessness).

It was also very important to the surveyed NRENs that awareness activities should not be on a one-off or short-term basis. They would like to see more properly planned and coordinated long-term programmes, lasting over a few years, as well as monthly activities, for example newsletters. An event similar to the CLAW crisis management exercise for NRENs but on different topics would be considered useful.

When asked about the role of GÉANT, NRENs responded that GÉANT should actively develop a security awareness programme. This should not simply include more materials, but also a toolkit and templates to enable NRENs to develop their own ‘awareness as a service’ for their members. It should additionally include support on adoption through Train the Trainer activities. Such a toolkit would also help NRENs further develop their internal programme.

## 3.3 Gap Analysis: Security Awareness Needs

Although most of the NRENs have some form cyber security awareness campaign or materials in place and some run successful internal and external activities, the majority still indicate that their awareness activity portfolio could be improved and more topics should be covered both for their staff (internal) and, even more so, for their members (external).

- The technical subjects of security awareness are generally well covered and most of these programmes are aimed at technical personnel. More focus should be given to non-technical

staff and especially management. It is also important to pay attention to the psychological and sociological aspects of cyber security when designing awareness activities.

- Universities and other NREN member organisations (as well as individual faculties within the universities) do not have the same needs, making it difficult for the NRENs to deliver unified security awareness services, and this is one of the reasons why such services are currently often either small and/or underdeveloped activities. However, it is important that topics related to data and privacy protection are addressed.
- The NRENs would like GÉANT to take an active role in developing and leading more security awareness activities. These activities should be long-term, regular (monthly) and include games, drills, films, etc.
- There is a need for Train the Trainer types of activities for the NRENs to run their own security awareness campaigns and joint events involving all NRENs to promote their cyber security awareness internally as well as to their member organisations.

# 4 Conclusions

The analysis of the NREN survey results show that although most of the NRENs have some security training and awareness initiatives in place, all of them would benefit from more joint community efforts.

There are a lot of suitable and publicly available security training programmes and materials online, as demonstrated through desktop research conducted as part of this report. The list of trainings and materials will be offered to the GÉANT community as a security training guide to be used to fill some of the gaps. However, it is important to note limitations, such as the lack of training materials in the Operational Network Security category, which is important to NRENs, and that three quarters of the listed trainings are dedicated to the technical personnel, when the NREN management, board and governance, and non-technical staff are the groups that were often mentioned as needing more support in this area.

Lack of funds and suitable training materials are some of the reasons why some NRENs do not have any security training in place. Accessibility and relevance will be taken into consideration by the team working on security trainings as the GN4-3 continues, aiming to address the issues of the NRENs with limited resources. Offering security trainings for their constituents is not a priority for most of the NRENs, but the security training guide and trainings developed as part of this project might be useful for the NREN members as well.

The situation is a little different when talking about security awareness, where many of the NRENs would like to offer ~~training~~ security awareness activities to their constituents and only a third of the surveyed organisations consider it to be out of scope because of a lack of funds or interest from their communities. The survey results show that the majority of the NRENs would like to have external security awareness campaigns targeting students. When asked about which groups could be better supported within the NRENs internally, almost half of the NRENs indicated their management.

Two thirds of the NRENs run internal security awareness programmes, covering a wide range of topics. The majority of the topics are better covered internally than externally, by the NRENs that also offer security awareness services to their members. Something that should be taken into consideration more when designing those programmes are the psychological and sociological aspects of cyber security.

However, what became evident when talking to the NRENs about both security training and awareness is that it is not only important to think about what we teach and what messages we try to get across, but also how we do it. There is a need to incorporate more diverse ways of teaching, such as games, drills, online trainings and webinars, train the trainer events, videos. Sharing best practises is also important, as there is already some content that can be shared between organisations, if it can

be translated to a different language. The NREN security community has a lot of expertise and knowledge that could be used to strengthen the security training and awareness efforts and GÉANT should play a role in coordinating those activities across Europe.

Based on the gap analyses, the GN4-3 WP8 Task 1 security training and awareness teams will prepare recommendations and plans for the future activities that will address the needs of the NRENs and assist them in securing their networks and organisations by investing in the weakest link of security – humans.

# Appendix A Overview of Security Training

Note:

- The table below is currently maintained on a wiki page [Wiki]. This is a temporary location and the intention is to order and move the information to a new security.geant.org site. Trainings offered by NRENs will also be included, as will information on which resources are open access.
- An overview of security awareness materials is under construction on a wiki page [Wiki2]. This information will also be moved to the new security.geant.org site.

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| GÉANT | https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS-I.aspx | TRANSITS-I | Live | Yes | 4 | Yes | Technical (Security) | Beginner |
| | https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS_II.aspx | TRANSITS-II | Live | Yes | 4 | Yes | Technical (Security) | Intermediate |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| ENISA | https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses | Malware Analysis and Memory Forensics | Live | No | 5 | Yes | Technical (Security) | Beginner |
| | | Mobile Threats and Incident Handling | Live | No | 1, 4 | Yes | Technical (Security) | Beginner |
| | | Introduction to Network Forensics | Live | No | 5 | Yes | Technical (Security) | Beginner / Intermediate |
| | | Incident Management: A Ransomware Walkthrough | Live | No | 4 | Yes | Technical (Security) | Beginner / Intermediate |
| RIPE NCC | https://www.ripe.net/support/training/courses/bgp | BGP Operation and Security Training | Live | No | 7 | Yes | Technical (Admin) | Intermediate |
| | https://www.ripe.net/support/training/material#ipv6-security | IPv6 Security Training | Live | No | 7 | Yes | Technical (Admin) | Intermediate |
| | https://www.ripe.net/support/training/material#advancedipv6 | Advanced IPv6 Training | Live | No | 7 | Yes | Technical (Admin) | Intermediate |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | https://www.ripe.net/support/training/material#DNSSEC | DNSSEC Training | Live | No | 7 | ? | Technical (Admin) | ? |
| FIRST | https://www.first.org/education/trainings#FIRST-CSIRT-Basic-Course | FIRST CSIRT Basic Course | Live | No | 4 | ? | Technical (Security) | Beginner |
| | https://www.first.org/education/trainings#FIRST-Threat-intel-Pipelines-Course | FIRST Threat intel Pipelines Course | Live | No | 3 | ? | Technical (Admin, Security) | Beginner |
| | https://www.first.org/education/trainings#DDoS-Mitigation-Fundamentals | DDoS Mitigation Fundamentals | Live | No | 7 | ? | Technical (Admin, Security) | Beginner |
| | https://www.first.org/education/trainings#Mastering-CVSSv3<br>https://learning.first.org/courses/course- | Mastering CVSSv3 | Live | No | 9 | Yes | Technical | Beginner |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | v1:FIRST+CVSSv3+2017/about | | | | | | | |
| | https://www.first.org/education/trainings#Incident-Handling-for-Policy-makers | Incident Handling for Policy makers | Live | No | 4 | ? | Managers | Beginner |
| | https://www.first.org/education/trainings#Conducting-Exercises-to-improve-Incident-Response | Conducting Exercises to improve Incident Response | Live | No | 4 | ? | Managers, Technical | Beginner |
| | https://www.first.org/education/trainings#IPv6-Security | IPv6 Security | Live | No | 1, 8 | Yes | Technical | Beginner |
| OpenHPI | https://open.hpi.de/courses/intsec2018 | Internet Security for Beginners | Online | Yes | 1 | ? | Users | Beginner |
| | https://open.hpi.de/courses/ws-privacy2016 | Social Media – What No One has Told You about Privacy | Online | Yes | 1, 6 | ? | Users | Beginner |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | https://open.hpi.de/courses/webtech2015 | Web Technologies | Online | Yes | 1 | ? | Users | Beginner |
| | https://open.hpi.de/courses/internetworking2014 | Internetworking with TCP/IP | Online | Yes | 1 | ? | Users, Technical (Admin) | Beginner |
| Coventry University | https://www.futurelearn.com/courses/basics-of-automative-cyber-security | Automotive Cyber Security: An Introduction | Online | Yes | 1 | ? | Technical (Developer) | Beginner |
| | https://www.futurelearn.com/courses/cryptography | An Introduction to Cryptography | Online | Yes | 1 | ? | Users, Technical | Beginner |
| | https://www.futurelearn.com/courses/network-security-basics | Basics of Network Security | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.futurelearn.com/courses/network-defence-management-overview | Network Defence Management Overview | Online | Yes | 1, 10 | ? | Managers | Beginner |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | https://www.futurelearn.com/courses/cyber-security-landscape | The Cyber Security Landscape | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.futurelearn.com/courses/security-operations | Security Operations | Online | Yes | 4 | ? | Managers, Technical | Beginner |
| | https://www.futurelearn.com/courses/cyber-security-in-the-software-development-life-cycle | Cyber Security in the Software Development Li fe Cycle | Online | Yes | 2, 6 | ? | Technical (Developers) | Beginner / Intermediate |
| | https://www.futurelearn.com/courses/ethical-hacking-an-introduction | Ethical Hacking: An Introduction | Online | Yes | 2 | ? | Technical | Intermediate |
| | https://www.futurelearn.com/courses/cyber-security | Cyber Security: Safety at Home, Online, in Life | Online | Yes | 1, 6 | ? | Technical | Beginner / Intermediate |
| Universidad Carlos III de Madrid | https://www.edx.org/course/cyber-security- | Cyber Security Basics: A | Online | Yes | 2, 3 | ? | Technical | Intermediate |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | basics-a-hands-on-approach | Hands-on Approach | | | | | | |
| KU Leuven | https://www.edx.org/course/web-security-fundamentals | Web Security Fundamentals | Online | Yes | 1, 3 | ? | Technical (Developer) | Beginner |
| OUNL (Open University Netherlands) | https://ou.edia.nl/courses/course-v1:OUNL+CG2019+2019_01/about | How Cryptography Keeps The Internet Secure | Online | ? | 1 | ? | Users | Beginner |
| TU Delft | https://www.edx.org/course/cyber-security-economics | Cyber Security Economics | Online | Yes | 1 | ? | Managers (Technical) | Intermediate |
| Tel Aviv University | https://www.edx.org/course/unlocking-information-security-part-i | Unlocking Information Security: Part Ⅰ | Online | Yes | 1 | ? | Technical (Security) | Intermediate |
| | https://www.edx.org/course/unlocking-information-security-part-2 | Unlocking Information Security: Part Ⅰ Ⅰ | Online | Yes | 2 | ? | Technical (Security) | Intermediate |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| University of London Royal Holloway | https://www.coursera.org/learn/information-security-data | Information Security: Context and Introduction | Online | Yes | 1 | ? | Users, Managers | Beginner |
| eit Digital | https://www.coursera.org/learn/cybersecurity | Cybersecurity for Identity Protection | Online | Yes | 1 | ? | Users | Beginner |
| | https://www.coursera.org/learn/security-privacy-big-data | Security and Privacy for Big Data - Part 1 | Online | Yes | 1, 6 | ? | Technical (Admin) | Beginner |
| | https://www.coursera.org/learn/security-privacy-big-data-protection | Security and Privacy for Big Data - Part 2 | Online | Yes | 1, 6 | ? | Technical (Admin) | Beginner |
| Palo Alto Networks | https://www.coursera.org/learn/cybersecurity-foundation | Palo Alto Networks Academy Foundation | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.coursera.org/learn/cybersecurity-gateway-1 | Palo Alto Networks Cybersecurity Gateway I | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.coursera.org/lea | Palo Alto Networks | Online | Yes | 1 | ? | Technical | Beginner |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | rn/cybersecurity-gateway-2 | Cybersecurity Gateway II | | | | | | |
| | https://www.coursera.org/learn/cybersecurity-essentials-1 | Palo Alto Networks Cybersecurity Essentials I | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.coursera.org/learn/cybersecurity-essentials-2 | Palo Alto Networks Cybersecurity Essentials II | Online | Yes | 1 | ? | Technical | Beginner |
| Google | https://www.coursera.org/learn/gcp-fundamentals | Google Cloud Platform Fundamentals: Core Infrastructure | Online | Yes | 1, 8 | ? | Technical | Intermediate |
| | https://www.coursera.org/learn/managing-security-in-google-cloud-platform | Managing Security in Google Cloud Platform | Online | Yes | 1, 8 | ? | Technical | Intermediate |
| | https://www.coursera.org/learn/mitigating-security-vulnerabilites-gcp | Managing Security Vulnerabilities on Google Cloud Platform | Online | Yes | 8, 9 | ? | Technical | Intermediate |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| Microsoft | https://www.edx.org/course/enterprise-security-fundamentals | Enterprise Security Fundamentals | Online | Yes | 1, 2 | ? | Technical | Intermediate |
| | https://www.edx.org/course/microsoft-azure-security-services | Microsoft Azure Security Services | Online | Yes | 6 | ? | Technical (Admin, Security) | Intermediate |
| IBM | https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks | Introduction to Cybersecurity Tools & Cyber Attacks | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.coursera.org/learn/cybersecurity-roles-processes-operating-system-security | Cybersecurity Roles, Processes & Operating System Security | Online | Yes | 1 | ? | Technical | Beginner |
| | https://www.coursera.org/learn/cybersecurity-compliance-framework-system-administration | Cybersecurity Compliance Framework & System Administration | Online | Yes | 1 | ? | Technical | Beginner |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | https://www.coursera.org/learn/network-security-database-vulnerabilities | Network Security & Database Vulnerabilities | Online | Yes | 1, 3 | ? | Technical | Beginner |
| SANS | https://www.sans.org/curricula/#cyber_defense | Cyber Defense Curriculum | Live | Yes | 1 | ? | Technical | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#system_administration | System Administration Curriculum | Live | Yes | 1 | ? | Technical (Admin) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#digital_forensic_investigations_and_media_exploitation | Digital Forensic Investigations and Media Exploitation Curriculum | Live | Yes | 5 | ? | Technical (Security) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#penetration_testing | Penetration Testing Curriculum | Live | Yes | 2 | ? | Technical (Security) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#incident_res | Incident Response and Threat Hunting Curriculum | Live | Yes | 4 | ? | Technical (Security) | Beginner, Intermediate, Advanced |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | ponse_and_threat_hunting | | | | | | | |
| | https://www.sans.org/curricula/#management | Management Curriculum | Live | Yes | 10 | ? | Managers (Technical) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#secure_software_development | Secure Software Development Curriculum | Live | Yes | 9 | ? | Technical (Security, Developer) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#audit | Audit Curriculum | Live | Yes | 2 | ? | Technical (Security) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#intrusion_analysis | Intrusion Analysis Curriculum | Live | Yes | 4, 5 | ? | Technical (Security) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#cyber_guardian | Cyber Guardian Curriculum | Live | Yes | 1 | ? | Technical (Admin, Security) | Beginner, Intermediate, Advanced |
| | https://www.sans.org/curricula/#legal | Legal Curriculum | Live | Yes | 10 | ? | Technical (Security) | Beginner, Intermediate, Advanced |
| (ISC)² | https://www.isc2.org/Certifications/SSCP | SSCP – Systems Security | Live, Online | Yes | 1, 3 | ? | Technical | Intermediate, Advanced |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | | Certified Practitioner | | | | | | |
| | https://www.isc2.org/Certifications/CISSP | CISSP – Certified Information Systems Security Professional | Live, Online | Yes | 1, 2 | ? | Technical | Intermediate, Advanced |
| | https://www.isc2.org/Certifications/CCSP | CCSP – Certified Cloud Security Professional | Live, Online | Yes | 8 | ? | Technical | Intermediate, Advanced |
| | https://www.isc2.org/Certifications/CSSLP | CSSLP – Certified Secure Software Lifecycle Professional | Live, Online | Yes | 9 | ? | Technical (Developer) | Intermediate, Advanced |
| | https://www.isc2.org/Certifications/CAP | CAP – Certified Authorisation Professional | Live, Online | Yes | 10 | ? | Technical | Intermediate, Advanced |
| Offensive Security Training | https://www.offensive-security.com/pwk-oscp/ | Penetration Testing with Kali Linux | Live, Online | Yes | 2 | Yes | Technical (Security) | Intermediate |
| | https://www.offensive- | Advanced Web Attacks and Exploitation | Live, Online | Yes | 2 | Yes | Technical (Security) | Advanced |

| Organiser | URL | Training Title | Availability | Certification possible | Training Category | In Use by NRENs | Target Audience | User Knowledge Level |
|---|---|---|---|---|---|---|---|---|
| | security.com/awae-oswe/ | | | | | | | |
| | https://www.offensive-security.com/ctp-osce/ | Cracking the Perimeter | Online | Yes | 2 | Yes | Technical (Security) | Advanced |
| | https://www.offensive-security.com/awe-osee/ | Advanced Windows Exploitation | Live | Yes | 2 | Yes | Technical (Security) | Advanced |
| | https://www.offensive-security.com/wifu-oswp/ | Wireless Attacks | Online | Yes | 2 | Yes | Technical (Security) | Advanced |
| HackerOne | https://www.hackerone.com/hacker101 | Hacker101 | Online | No | 3 | ? | Technical (Security) | Intermediate / Advanced |

Table A.1: Courses and training materials currently available to NRENs

# Appendix B Survey

| | | |
|---|---|---|
| **Part 1** | **Questions about the NREN** | |
| | | |
| Q 1.1 | Number of users working directly for your NRENs organisation? | |
| | *(specify, a rough estimate is sufficient)* | |
| | | |
| Q 1.2 | Number of users in your NRENs member organisations? | |
| | *(specify, a rough estimate is sufficient)* | |

| | | |
|---|---|---|
| **Part 2** | **Questions about the IT security awareness program** | |
| | | |
| | **General** | |
| | | |
| Q 2.1 | Does your organisation supply or recommend an IT security awareness program? | |
| | | Yes/No |

| | | |
|---|---|---|
| Q 2.2 | If not, can you give reasons why? | |
| | *(check, specify)* | |
| | No suitable awareness material found | Yes/No |
| | Lack of funds | Yes/No |
| | Organisations members haven‘t specified a need | Yes/No |

| | | |
|---|---|---|
| | Other reasons *(specify)* | |

| | | |
|---|---|---|
| Q 2.3 | What role should GÉANT take with regards to IT security awareness programs? (state all that apply) | |
| | Actively develop an IT security awareness program for its members | Yes/No |
| | Point members to existing IT security awareness programs | Yes/No |
| | Stay out of this area | Yes/No |
| | Other reasons *(specify)* | |

| | | |
|---|---|---|
| Q 2.4 | How often are your internal awareness programs run per year? | |
| | *(specify # of times/year)* | |

| | | |
|---|---|---|
| Q 2.5 | Is this frequencey sufficient for your requirements? | |
| | Could be more often *(specify # of times/year)* | |
| | Could be less often *(specifiy # of times/year)* | |

| | | |
|---|---|---|
| Q 2.6 | How often are the awareness programs for your member organisations run per year? | |
| | *(specify # of times/year)* | |

| | | |
|---|---|---|
| Q 2.7 | Is this frequencey sufficient for your requirements? | |
| | Could be more often (specify # of times/year) | |
| | Could be less often (specifiy # of times/year) | |

| | | | | | |
|---|---|---|---|---|---|
| | **Identification of gaps in topic coverage** | | | | |
| | | | | | |
| Q 2.8 | How well are you satisfied with your organisations internal IT security awareness programs? | | | | |
| | Topic | Well covered | Needs Improvement | Not covered | If „needs improvement“, what kind of improvement? |
| | „You are the target“ | | | | |
| | Social Engineering | | | | |
| | Email and Instant Messaging | | | | |
| | Social Networking | | | | |
| | Browsers | | | | |
| | Passwords | | | | |
| | Encryption | | | | |
| | Data Safety | | | | |
| | Mobile Devices/Smartphones/ Laptops | | | | |
| | Monitoring/Acceptable Use Policy (AUP) | | | | |
| | Hacked/Incident Response | | | | |
| | Physical Security | | | | |
| | Licensing | | | | |
| | System configuration management | | | | |

| | | |
|---|---|---|
| Q 2.9 | Are there additional topics you'd like to have covered in an IT security awareness program for your organisation internally? (i.e. not in the list above) | |
| | *(specify the most important ones)* | Topics |
| | | |
| | | |

| | | | | | |
|---|---|---|---|---|---|
| Q 2.10 | How well are you satisfied with the IT security awareness programs your member organisations use? | | | | |
| | Topic | Well covered | Needs Improvement | Not covered | If „needs improvement", what kind of improvement? |
| | „You are the target" | | | | |
| | Social Engineering | | | | |
| | Email and Instant Messaging | | | | |
| | Social Networking | | | | |
| | Browsers | | | | |
| | Passwords | | | | |
| | Encryption | | | | |
| | Data Safety | | | | |
| | Mobile Devices/Smartphones/ Laptops | | | | |
| | Monitoring/Acceptable Use Policy (AUP) | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Hacked/Incident Response | | | | |
| | Physical Security | | | | |
| | Licensing | | | | |
| | System configuration management | | | | |

| | | |
|---|---|---|
| Q 2.11 | Are there additional topics you'd like to have covered in an IT security awareness program for your member organisations? (i.e. not in the list above) | |
| | *(specify the most important ones)* | Topics |
| | | |
| | | |

| | | | |
|---|---|---|---|
| | **Identification of gaps in target audience group coverage** | | |
| | | | |
| Q 2.12 | What target audience groups are covered by your organisations internal IT security awareness programs? | | |
| | *(specify the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| Q 2.13 | What target audience groups could be better supported by your organisations internal IT security awareness programs? | | |
| | *(specify the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| Q 2.14 | What target audience groups are covered by the IT security awareness programs for your member organisations? | | |
| | *(specify the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| Q 2.15 | What target audience groups could be better supported by IT security awareness programs for your member organisations? | | |
| | *(specify the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | |
|---|---|---|
| | **Identification of other gaps** | |
| | | |
| Q 2.16 | Any other suggestions for an IT security awareness program? | |
| | *(specify)* | Suggestions |
| | | |

| | | |
|---|---|---|
| **Part 3** | **Questions about the IT security training program** | |
| | | |
| | **General** | |
| | | |
| Q 3.1 | Does your organisation supply or recommend IT security trainings? | |
| | *(if yes, specify)* | |

| | | |
|---|---|---|
| Q 3.2 | If not, can you give reasons why not? (check, specify) | |
| | No suitable training material found | Yes/No |
| | Lack of funds | Yes/No |
| | Organisations members haven‘t specified a need | Yes/No |
| | Other reasons *(specify)* | |

| | | |
|---|---|---|
| Q 3.3 | What role should GÉANT take with regards to IT security training programs? (state all that apply) | |
| | Actively develop an IT security training program for its members | Yes/No |
| | Point members to existing IT security training programs | Yes/No |
| | Stay out of this area | Yes/No |
| | Other reasons (specify) | |

| | | |
|---|---|---|
| | **Identification of gaps in topic coverage** | |
| | | |
| Q 3.4 | If you have an internal IT security training program, what topics are covered by it? | |
| | *(specify only the ones most important)* | Topics |
| | | |
| | | |

| | | |
|---|---|---|
| Q 3.5 | What are topics you‘d like to have covered in an IT security training program for your internal use? | |
| | *(specify only the ones most important)* | Topics |
| | | |

| | | |
|---|---|---|
| | | |

| | | |
|---|---|---|
| Q 3.6 | If you have an IT security training program for your member organisations, what topics are covered by it? | |
| | *(specify only the ones most important)* | Topics |
| | | |
| | | |

| | | |
|---|---|---|
| Q 3.7 | What are topics you'd like to have covered in an IT security training program for your member organisations? | |
| | *(specify only the ones most important)* | Topics |
| | | |
| | | |

| | | | |
|---|---|---|---|
| | **Identification of gaps in target audience group coverage** | | |
| | | | |
| Q 3.8 | What target audience groups are covered by the IT security trainings currently in use for your organisation internally? | | |
| | *(specifiy the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| Q 3.9 | What target audience groups could be better supported by IT security awareness programs for your organisation internally? | | |
| | *(specifiy the most important ones)* | Target audience groups | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| Q 3.10 | What target audience groups are covered by the IT security trainings currently in use for your member organisations? | | |
| | *(specifiy the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| Q 3.11 | What target audience groups could be better supported by IT security awareness programs for your member organisations? | | |
| | *(specifiy the most important ones)* | Target audience groups | |
| | | | |
| | | | |

| | | |
|---|---|---|
| | **Identification of other gaps** | |
| | | |
| Q 3.12 | Any other suggestions for IT security trainings? | |
| | *(specify)* | Suggestions |
| | | |

# References


| | |
|---|---|
| **[Cybersecurity]** | EC, Joint Communication to the EP and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017, p. 2 |
| **[ENISA]** | ENISA (2017) Stock taking of information security training needs in critical sectors, ISBN: 978-92-9204-231-8, DOI: 10.2824/521757 |
| **[Wiki]** | https://wiki.geant.org/pages/viewpage.action?spaceKey=gn43wp8&title=Table+of+Security+Training+Courses (Note that this is a temporary location and the intention is to order and move the information to a new security.geant.org site) |
| **[Wiki2]** | https://wiki.geant.org/pages/viewpage.action?pageId=126982484 |

# Glossary

| | |
|---|---|
| **DDoS** | Distributed Denial-of-Service |
| **DNS** | Domain Name System |
| **GDPR** | General Data Protection Regulation |
| **ICT** | Information and Communications Technology |
| **NREN** | National Research and Education Network |
| **R&E** | Research and Education |
| **SDL** | Software Development Livecycle |