01-02-2024

Status of Cyber Security Awareness within National Research and Education Networks

Grant Agreement No.:	101100680
Work Package:	WP8
Task Item:	Task 2
Nature of Document:	Background
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT Association
Document ID:	GN5-1-24-33a44e

Authors:	Davina Luyten (Belnet), Charlie van Genuchten (SURF), Rosanna Norman (GÉANT), Mark Tysom (Jisc), Marina Dimić Vugec (CARNET)

Abstract

This report describes the outcomes of a survey conducted by GN5-1 Work Package 8, Task 2 Human Factor (WP8 T2), subtask Awareness, on the status of cyber security awareness within the National Research and Education Networks.

Table of Contents

Table of Figures

Executive Summary

This report describes the outcomes of a survey (Appendix B) conducted by GN5-1 Work Package 8, Task 2 Human Factor (WP8 T2), subtask Awareness, on the status of cyber security awareness within the National Research and Education Networks.

Security awareness relates to the measure in which employees are aware of cyber threats and know what they can do to mitigate these risks. The majority of surveyed NRENs consider the "human factor" to be a key element of cyber security and are actively taking actions to train their employees. As expected, the maturity of NRENs in this area was found to vary widely, but overall NRENs are striving to build a strong security culture in their organisations.

How NRENs approach their security awareness programs also varies. Where some rely on ad hoc actions for a general audience, others already have a risk-based approach involving tailored strategies for different target audiences. The channels used also vary widely, ranging from classic training methods to awareness games.

We noted that most NRENs have limited resources for internal security awareness, with only a few having a dedicated FTE to tackle this challenge. Most internal awareness officers are part of the Security or CERT teams within their organisation and coordinate with other departments such as Marketing & Communication.

In general, NRENs can still improve their existing plans by applying metrics to measure the impact and success of their awareness programmes.

Finally, regarding external awareness activities, most NRENs help their communities to tackle security challenges by providing them with communication materials and e-learning, and organising security events and conferences, etc. The same difference in maturity as for the internal awareness part is also evident in these initiatives.

A wealth of ready-to-use security materials were developed in previous GÉANT projects, which the Awareness subtask in GN5-1 WP8 T2 intends to build on in the future so that NRENs can have a wide range of materials at their disposal.

While it will be difficult to have a direct impact on some of the challenges that NRENs face where limited resources for security awareness are the issue, the subtask is making efforts to raise awareness of the human factor in security in the community, for example at the GÉANT Symposium, TNC, security conferences, etc.

The Awareness subtask will continue to work towards its objective of helping NRENs set up and improve their awareness programmes in order to strengthen their resilience against security incidents, tailoring its support to meet the different needs and capabilities of the diverse GÉANT community.

To this end, the Security Awareness survey should be run on a regular basis (e.g. biannually) to monitor NRENs' progress in this area.

1 Introduction

Human error is one of the major security threats that organisations face. More than ever, it is important for organisations to protect themselves against cybercrime not only with adequate technical security measures, but also by raising awareness and training their employees. This also applies to National Research and Education Networks (NRENs).

This report describes the outcome of a survey conducted by GN5-1 Work Package 8, Task 2 Human Factor (WP8 T2), subtask Awareness, on the status of cyber security awareness within the National Research and Education Networks. In this report, the subtask aims to investigate the status of security awareness within the NRENs and define concrete steps for further actions for the Awareness subtask.

In the context of the previous GN4-3 project, WP8 – T1 Business Continuity started laying the groundwork for cyber security awareness on which the present project will continue to build. More specifically, in 2019 an initial campaign was started with a small number of NRENs, which from 2020 onwards became a yearly large-scale awareness campaign for the European R&E community in conjunction with Cyber Security Month [CSM]. The GN5-1 project builds upon this work by increasing the number of cyber security awareness initiatives for different target groups (NRENs, constituents and end users) and aims to encourage and help NRENs to set up awareness initiatives or to improve their existing programmes.

This document is structured as follows:

- Section 2 presents an overview of the methodology used for the survey questionnaire and of the respondents and interviewees.
- Section 3 provides an overview of the NRENs' maturity in terms of internal security awareness and presents key findings on their internal awareness programmes, formats, resources and the needs of the NREN community.
- Section 4 covers the NRENs' external awareness initiatives, target groups, formats and the resources available.
- Finally, Section 5 draws some overall conclusions and presents next steps.
- A set of two appendices respectively present the overview of the NRENs involved in the CSM campaigns and in the awareness survey/interviews (Appendix A) and the results of the Security Awareness Survey (Appendix B).

2 Approach

This section presents an overview of the methodology used for the survey questionnaire and of the survey respondents and interviewees.

2.1 Survey Methodology

To prepare the questionnaire (see Appendix B), the GN5-1 WP8 Subtask relied on the SANS Security Awareness Maturity Model [SANS]. Established in 2011 through a coordinated effort by over 200 security awareness officers, this model has become the industry standard which organisations not only use to benchmark the maturity of their programme, but also leverage as a strategic roadmap to plan and communicate the impact of their programme. The questions were designed in such a way that the outcome allows a view of the NRENs' maturity with regard to their internal awareness programmes.

As we also wanted to find out what the NRENs are doing in terms of external security awareness, the second part of the survey was specifically about awareness initiatives for external stakeholders (member institutions and their end users, but also the 'general public').

The GN5-1 WP8 Subtask sent this survey to different NRENs and followed it up with in-depth interviews of approximately half of the surveyed NRENs to get more background information.

2.2 Survey Respondents and Interviewees

The GN5-1 WP8 T2 Awareness subtask reached out to 28 NRENs. The selection was mainly made on the basis of those NRENs the subtask participants had already worked with in recent years as part of the CSM campaigns, and had the relevant contacts for within these organisations, therefore could assume to achieve a good response rate from.

Besides, the team reached out to a few other NRENs who were not involved in CSM, but for which alternative contact people could be identified through the GÉANT communications team.

This means that there is a bias in respondents, as they are mainly NRENs that are already interested in the topic of security awareness.

In the end, 25 organisations responded to the survey – 24 NRENs plus GÉANT – of which only 1 had never participated in the GÉANT Cyber Security Month (see Appendix A).

Participation in the CSM campaigns can take different forms: writing content (such as a blog post, story or case study), giving an online talk for the webinar programme and/or active promotion and dissemination of the CSM campaign within the local community.

In terms of geographic spread, 11 North/West European, 6 Eastern European and 7 Southern European NRENs participated in the survey.

The survey was filled out by NREN staff with different types of profiles: security experts, CISOs, network coordinators, communication officers.

Half of the surveyed NRENs (12) took part in the in-depth interviews. These were all NRENs who already have an awareness programme in place. The interviewees were the same person(s) who filled out the survey.

The NRENs surveyed/interviewed were very different in scale and scope. There were NRENs with less than 20 people, and NRENs with more than 300 employees. This also means that the size and complexity of their target group for internal security awareness is very different. The same goes for the size and complexity of their external target groups, as NRENs serve different types of communities. Another difference is that some of the surveyed NRENs operate the national CERT for their country, often including specific tasks regarding external awareness, such as the organisation of national campaigns.

Regarding the NRENs that did not participate in the survey, it is assumed that they run few internal awareness initiatives. This assumption is based on the fact that most of them have never been involved in CSM campaigns in the past. However, this needs further investigation. An action point for the Awareness subtask would be to identify the relevant contact persons within these NRENs (see Section 5 Conclusions and Recommendations).

3 Internal Security Awareness: Status of the NRENs

3.1 Overview

Based on the survey responses, we were able to divide the NRENs into the different 'stages' according to the SANS Security Awareness Model [SANS]. This division does not imply any value judgment, but does provide a good overview of where the NRENs are positioned in terms of internal awareness. As expected, there are big differences between NRENs.

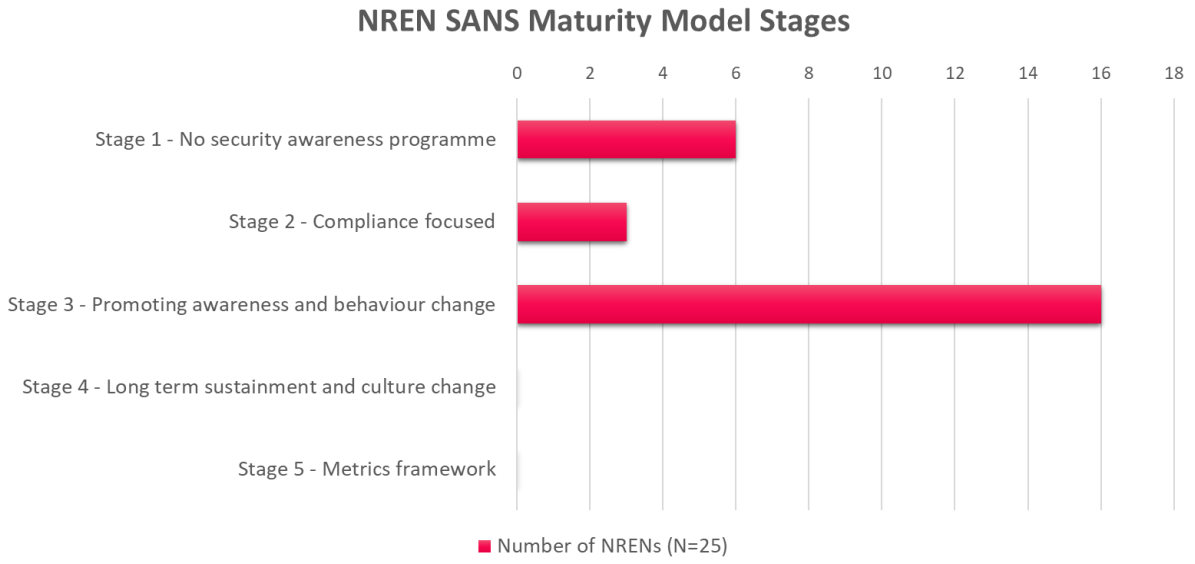


Figure 3.1: SANS Maturity Model stages of surveyed NRENs (total 25 NRENs)

Stage 1: No security awareness programme (6 NRENs)

SANS definition: *"In this stage a security awareness programme does not exist in any capacity. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organisation, do not know or follow organisation policies, and easily fall victim to attacks."*

6 out of 25 surveyed NRENs (24%) indicated that no internal awareness programme has been set up within their organisation so far. Asked about the reason(s) for this, 4 NRENs cited as the main reason a lack of resources. On the other hand, 3 of the NRENs have concrete plans to introduce an awareness programme, and 1 is in the process of introducing an ISMS. Some of the NRENs in this stage are thus already taking steps to move to stage 2.

Note that the description above is the SANS definition. We assume that the employees of the NRENs at this stage nevertheless already have some basic security knowledge, for example from 'external' campaigns in their country from national authorities, banks, etc. Also, as our survey did not test the knowledge and behaviour of employees, we cannot state that they are completely unaware.

Stage 2: Compliance focused (3 NRENs)

SANS definition: *"In this stage the programme is designed primarily to meet specific compliance or audit requirements. Training is limited to being offered on an annual or ad-hoc basis. Employees are unsure of organisational policies and/or their role in protecting their organisation's information assets."*

3 out of the 25 surveyed NRENs (12%) fall under this category. Within these NRENs, awareness initiatives are run on an ad-hoc basis and are often limited to onboarding initiatives for new employees. Apart from this, there is little communication encouraging secure behaviours. Also, any awareness programmes are mainly carried out by someone within the NREN security team who has other (primary) responsibilities, without much coordination or collaboration with other departments such as HR or Communications. The respondents further indicated that leadership involvement is rather limited and employees are insufficiently aware of the internal security procedures to report incidents. On the other hand, all 3 NRENs in this category are already taking steps to raise their awareness programmes to a higher level.

Stage 3: Promoting awareness and behaviour change (16 NRENs)

SANS definition: *"In this stage the programme identifies the target groups and training topics that have the greatest impact in managing human risk and ultimately supporting the organisation's mission. The programme goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behaviour change. As a result, people understand and follow organisation policies and actively recognise, prevent, and report incidents."*

The majority of the surveyed NRENs (16 out of 25, i.e. 64 %) have an internal awareness programme which corresponds to SANS Stage 3. However, their approaches vary greatly between them (see chapter 3.2). Not all NRENs in this stage already have a structured and formal programme. In terms of resources, most NRENs have a collaboration between the security team and the communications team in place to run the awareness programme. However the members of these teams often combine these tasks with other (primary) responsibilities. The NRENs in this stage indicated that awareness is considered part of their organisation's overall security effort. They combine training and e-learning with other initiatives such as simulated phishing campaigns.

Stage 4: Long-term sustainment and culture change (0 NRENs)

SANS definition: *"The programme has the processes, resources, and leadership support in place for a long-term life cycle, including (at a minimum) an annual review and update of the programme. As a result, the programme is an established part of the organisation's culture and is current and engaging. The programme has gone beyond changing behaviour and is changing people's beliefs, attitudes, and perceptions of security."*

Although none of the NRENs surveyed / interviewed are at this stage yet, 13 NRENs are already taking steps towards making their awareness programme sustainable over the long term. These efforts include for example an active review and update of the programme on an annual basis, the use of different training methods for different target groups and the use of gamification and/or security ambassadorship.

Stage 5: Metrics framework (0 NRENs)

SANS definition: *"The programme has a robust metrics framework aligned with the organisation's mission to track progress and measure impact. As a result, the programme is continuously improving and is able to*

demonstrate return on investment. Metrics are an important part of every stage, and this level simply reinforces that to truly have a mature programme, you must be able to demonstrate value to the organisation."

None of the surveyed NRENs have an awareness programme in SANS Stage 5.

3.2 Highlights

The highlights presented below relate to the surveyed NRENs that already have an ad-hoc (Stage 2 of the SANS Awareness Model) or formal (from Stage 3 of the SANS model) internal awareness programme (19 in total).

Awareness programmes are risk-based and getting more mature with a targeted approach

In the first part of the survey, we wanted to find out for how long NRENs have been running an internal awareness programme and what the main objective of their programme is. We also wanted to understand if prior to setting up the programme a risk analysis was conducted and how the programme was adapted to new risks and threats.

Half of the NRENs (10) have been running their internal awareness programmes for between 1 and 3 years, meaning they have already built up some expertise in this domain, while 7 others started their programmes more than 3 years ago.

Asked the main purpose of their programme, 17 out of 19 NRENs responded that they aim to build a strong security culture within their organisation. One NREN indicated that their main objective is to meet legal requirements. One other NREN responded that it does not have a specific goal set for its awareness programme.

A risk assessment is a powerful tool to identify gaps in the security knowledge and behaviour of employees. It allows organisations to focus on the right training for the right people. The majority of the NRENs indicated that they have identified the top human risks prior to developing their awareness programme and also adapt their programme to new risks such as emerging phishing techniques or QR code fraud.

"A risk analysis was conducted prior to rolling out various security initiatives. For example, high-risk/value users (e.g. with significant budget approval status) were the first to benefit from multi factor authentication on their accounts."

9 out of 19 NRENs have a different approach for different target groups, meaning that training is adapted to the specific requirements of their employees. For example, in-depth training on processing personal data is organised for staff working in the HR department, whereas financial departments are trained to recognise phishing mails with fake invoices. 7 of out 19 NRENs also provide specific skills-based training opportunities for their IT and developers groups.

Different formats are used to involve employees

Regarding the formats used in their internal awareness programmes, we see that NRENs combine classical training methods, such as training sessions with an instructor (78%) and e-learning (72 %), with more 'engaging' initiatives such as awareness games (61 %) or security ambassadorship (39 %).

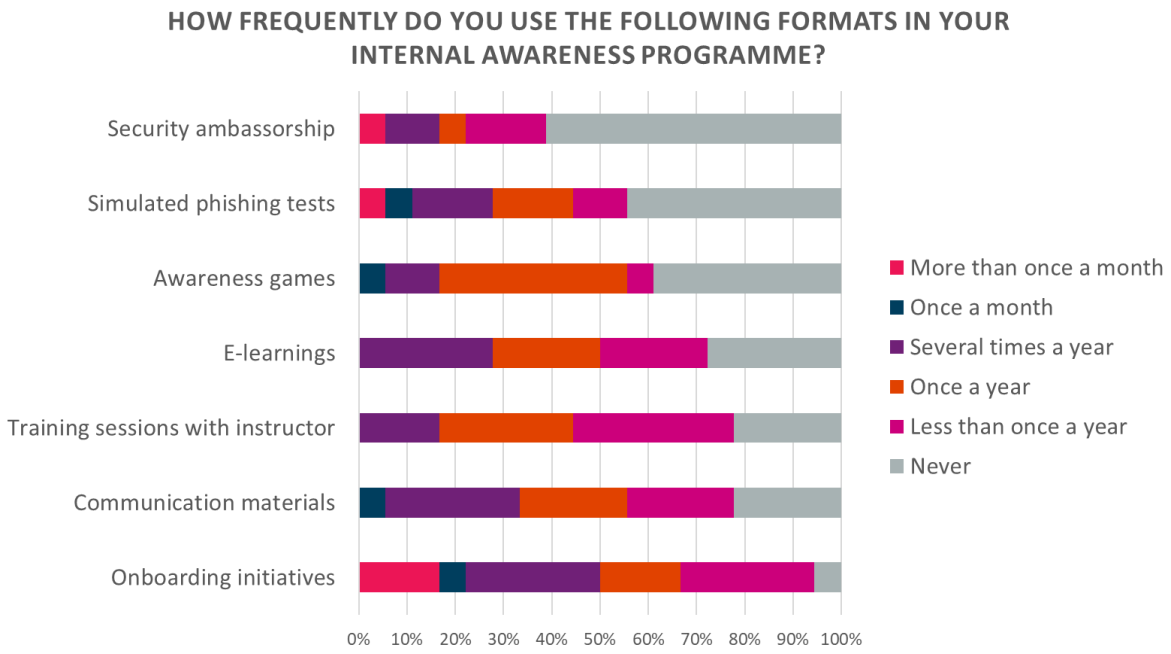


Figure 3.2: Materials used by NRENs in their internal security awareness programmes (total 25 NRENs)

With the exception of one NREN, all respondents run specific awareness training for new employees within their organisations. These onboarding initiatives vary in frequency from once a year to several times a month. We assume this is strongly linked to the NRENs' size and the number of new employees that join them.

A small majority of respondents (10 out of 19) indicated that they use simulated phishing tests to raise awareness among their employees. It would be interesting to further investigate this point as opinions vary on the effectiveness of this kind of tests.

By adding gamification elements in cyber security awareness training, organisations can increase the engagement and involvement of their users and improve their learning experience. 11 out of 19 NRENs already include awareness games in their training programmes.

Other learning formats mentioned by NRENs are conferences and 'lunch-and-learn' sessions (interactive sessions with expert speakers held during lunch).

"Our training programme is quite recent and we are also learning with it. We expect to have a better overview in the coming year and also to improve it according to our internal needs."

Internal security awareness is usually the task of the Security / CERT team

Since most NRENs are rather small to medium-sized organisations, it is not surprising that the person(s) responsible for the internal awareness programme combine(s) this work with other, often primary, responsibilities. Only three out of 19 NRENs have at least one dedicated FTE for internal security awareness.

Asked in which department the internal awareness officer(s) work, most responded that they are part of the CERT or the Security team of their organisation. A majority (68%) of the NRENs uses an interdisciplinary approach for internal awareness, meaning that the person in the CERT/Security team is coordinating activities with other internal stakeholders. These include experts from IT support, Marketing & Communication or Legal teams, but

also from general management. On the other hand, four out of 19 NRENs have yet to set up a collaboration between their security and communications department for internal awareness-raising activities.

"The security officer and the communications department want to tackle the issue together in the future."

NRENs were asked to rate on a scale from 0 to 100 to what extent their management is involved in the internal awareness programme. The majority (79%) finds their management is (strongly) involved, giving scores above 60 and even 100. On the other hand, management involvement is considered rather low by 21% of the surveyed NRENs.

Limited use of metrics to measure the effectiveness of internal awareness programmes

Metrics are one of the key elements of a successful awareness programme. These are crucial to measure the impact of a programme in order to be able to continuously improve it and to demonstrate return on investment. Metrics are part of every stage of the SANS Security Awareness Model but they vary from pure quantitative metrics such as the number of people who have completed training (stage 2) to a full strategic framework where both quantitative and qualitative metrics are collected and combined into a single dashboard (stage 5).

Almost half of the NRENs (9 out of 19 NRENs) collect metrics to measure the success of their awareness programme. All but one of these also report these metrics to their management. However, this also means that a small majority of NRENs currently does not collect any statistics about the effectiveness of their programme.

As regards which type of metrics are collected, we noted that these are mostly those that measure people's involvement in a quantitative way (number of participants in trainings or surveys), their behaviour (number of reported incidents, click-through rates of phishing simulation tests), and their knowledge (scores of post-training assessments). However most NRENs do not yet measure people's attitudes, perceptions and beliefs regarding information security. As most NRENs are in stage 3 of the SANS Security Awareness Model, collecting this kind of metrics is a required step to enable them to reach the next stage.

Need for more communication on how to report incidents

To effectively manage human risk, it is important for employees to feel confident asking security-related questions and to know how to report security risks or incidents.

All surveyed NRENs (25) were asked if they have an internal procedure to report security incidents. Most of the NRENs (23) confirmed that they have such a procedure in place. In some cases, these procedures are not formally documented. Some NRENs use nudging techniques to steer people in the right direction and help them follow the procedures, such as a phish button in their email client to easily report suspicious emails.

However, 10 out of the 23 NRENs state that their employees are insufficiently aware of the existing procedures, and thus more communication / awareness is needed on how to report incidents.

"We do have a procedure, unfortunately I observe that not everyone is aware of the channels that must be used to report a security incident."

Asked about the existing security policies within their organisation, most surveyed NRENs responded that they have a security policy (21) and an acceptable use policy (19) in place. A majority also have an email policy (15),

while a minority have an awareness training policy in place (9) which specifies the scope and purpose of their information security awareness and training program and defines what is expected from employees.

Other procedures / policies mentioned concern passwords, privacy, BCP, crisis management, clean desk and GPDR. Some NRENs are [ISO27001] certified thus have all the policies in place required to obtain this standard.

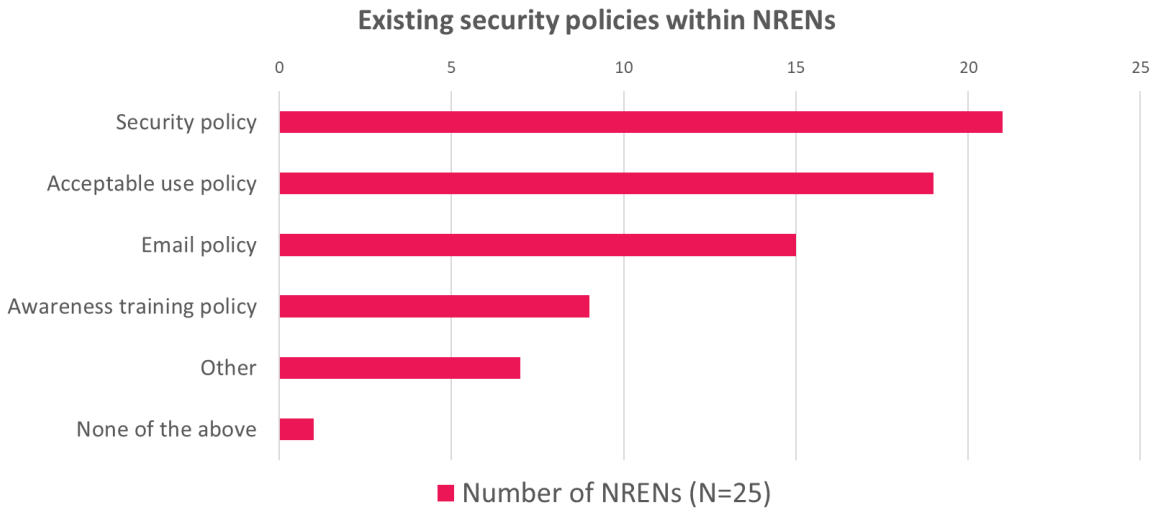


Figure 3.3: Security policies in place at surveyed NRENs (total 25 NRENs)

3.3 Needs

We wanted to know how the Awareness subtask in WP8 T2 can support NRENs with their internal security awareness. Overall, the results of the survey show that the community is most interested in sharing best practices and experiences with other NRENs (84%) and in receiving ready-to-use awareness materials (76%).

32% of the NRENs would like to receive training on how to set up (or improve) their programme. Regarding training sessions for end users, opinions vary as, as mentioned, some NRENs already include this in their service offering. However, 48% are still interested in having this developed by GÉANT.

The topics / risks that NRENs consider most relevant to include in their awareness programme are password security, data protection and privacy and phishing/vishing/smishing. These are in line with the results of previous surveys when NRENs were asked on which topics in particular the GÉANT Cyber Security Month campaigns should focus.

4 NREN External Security Awareness Initiatives

Most NRENs provide specific security services to their member institutions and end users. Given that the human factor represents a significant risk, it makes sense for NRENs to include security awareness in their external service offering. Therefore, in the second part of the survey, we surveyed NRENs about their security awareness initiatives towards external stakeholders.

4.1 Highlights

Most NRENs have external awareness-raising activities

First, we wanted to find out whether NRENs support their member institutions and/or end users in the area of security awareness. The vast majority of NRENs (19 out of 25) take actions to sensitise external stakeholders on the topic of security. 14 of these do so in an ad-hoc manner, while 5 NRENs run a structured programme. The remaining 6 NRENs indicated that they do not conduct any external awareness initiatives. The main reason mentioned for this is a lack of resources. These 6 NRENs vary greatly in terms of the number of end users, so they are not just smaller NRENs.

Of the 19 NRENs with an external awareness programme, 16 indicated that they have been engaged in external awareness initiatives for more than three years.

"We have a toolkit and a community, our members always know where to ask questions and find material."

With the exception of two NRENs, we found that all organisations with an internal awareness programme are also implementing external initiatives. On the other hand, two NRENs that are already engaged in external awareness indicated that they do not (yet) have a programme internally. Overall, four of the 25 surveyed NRENs surveyed are not engaged in security awareness, either internally or externally.

NREN constituents are the most important target groups

When asked about the target audience of their external awareness initiatives, all NRENs responded that their focus is on the people working in their connected institutions. 12 out of 19 NRENs also try to raise awareness among the end users connected to their networks, such as students in higher education. Some NRENs (4) even have a broader scope and target every citizen/internet user in their country. We note that these NRENs are involved in or operate the national CERT for their country, including awareness-raising activities for a broad public.

A variety of formats, including awareness games

Regarding external awareness-raising activities, we see that NRENs use a wide range of formats. Most NRENs (14 out of 19) organise events such as conferences or workshops for their constituents. Other commonly used

formats are specific awareness campaigns (13 NRENs), for example those taking place during the European Cyber Security Month, and the distribution of communication materials such as flyers, videos or posters (11 NRENs).

6 NRENs make e-learnings available to their members or end-users, and the same number of NRENs have developed awareness games for their community. Other formats mentioned are an annual awareness survey, a security-related news service, and the creation of an awareness community to share ideas and best practices.

An interdisciplinary approach

In line with the previous chapter, we asked the NRENs how many resources they have available to implement their external awareness-raising activities.

As is the case for internal awareness, the person responsible for external awareness activities is in most cases (12 out of 19 NRENs) combining this work with other (primary) responsibilities. Some NRENs precised that the same person is working on both internal and external awareness activities.

However, 7 out of 19 NRENs do have at least one dedicated FTE for external awareness which is significantly more than for internal awareness (where only 3 out of 19 NRENs have a dedicated FTE).

Asked in which department the external awareness officer(s) work, almost all (17 out of 19) responded that they are part of the CERT or Security team of their organisation. One NREN assigns this task to the Marketing & Communications department and one NREN to the Product Management team.

A majority (68%) of the NRENs uses an interdisciplinary approach for external awareness, meaning that the person in the CERT/Security team is coordinating activities with other internal stakeholders. These include experts from IT support, NOC, Marketing & Communication, Trust & Identity or Legal teams, but also from general management.

4.2 Needs

We wanted to know how the Awareness subtask in WP8 T2 can support NRENs with their external security awareness. NRENs express the greatest interest in sharing best practices within the GÉANT community (84%). There is less interest in teaching connected organisations how to set-up their own awareness programme (50%) and training for end users (37,5%).

The topics / risks that NRENs consider most relevant to include in their external awareness programmes are data protection and privacy, phishing/vishing/smishing, and ransomware. All these topics have already been addressed during the previous GÉANT Cyber Security Month campaigns.

5 Conclusions

The outcomes of the security awareness survey carried out by the Awareness subtask in GN5-1 WP8 reveal that the maturity of NRENs in terms of internal and external awareness varies widely, although the maturity status of NRENs that did not participate in the survey remains uncertain.

NRENs indicate that they wish to share good practices and experiences with each other so that those organisations that are less mature can learn from others who are already at a further stage of the SANS Awareness Model. This model can serve as a guideline to develop training/workshops for the NRENs to take their programmes to the next level.

NRENs have also requested communications materials they can easily adapt themselves and deploy in their own organisations.

There are some challenges that NRENs face where it will be difficult for the Awareness subtask to have a direct impact, for example where there is a lack of resources for security awareness. Nevertheless, efforts are being made to raise awareness of the human factor in security among the community, for example at the GÉANT Symposium, TNC, security conferences, etc.

The Awareness subtask remains committed to its objective of helping NRENs to set up and improve their awareness programmes in order to strengthen their resilience against security incidents. Support will also be tailored so as to meet the different needs and capabilities of the diverse GÉANT community.

5.1 Next Steps

Based on the outcomes of the survey, the following actions are planned:

- The Awareness Subtask in WP8 T2 aims to build an active community of awareness officers who regularly come together (online or physically) to discuss insights in security awareness, share the results of their programmes, exchange ideas, etc. Within this community, the subtask can provide tools and training to help starting NRENs to set up their programmes and others to take their programmes to the next stage. Ideas for training topics include:
    - identifying target groups within your organisation and their specific risks in the area of privacy and security,
    - mapping behavioural factors and learning how to encourage desired behaviour from your users,
    - and setting up metrics to measure the effectiveness of your awareness programme.
- The Awareness subtask will attempt to identify the relevant contact persons within the NRENs that did not participate in the survey, starting from the strategic (CEO) level. Cross-checks can be carried out to verify if NRENs who did not complete the survey have attended any GÉANT security meetings/workshops to identify the most appropriate contacts. The long-term goal is to have these NRENs also join the awareness community.
- A list of all existing security materials and resources developed in previous projects will be compiled and made available to the community in one place, ensuring that NRENs are aware of these materials and can easily access them. The GÉANT Security website seems to be the best platform for this awareness repository and, if a more protected access should be needed, could be linked to the GÉANT

Wiki. Furthermore, the Awareness subtask will continue to develop white-labelled materials that can easily be adapted and reused by NRENs and their constituents. These materials may form part of the yearly Cyber Security Month campaign, but could also be linked to specific events throughout the year (Safer Internet Day, World Back-up Day, etc.). For example, last year, the Business Continuity Task developed a first awareness game for the community ("Security Trumps") in collaboration with the Awareness subtask, which has been received very well. The subtask will therefore investigate if other initiatives can be developed based on the concept of gamification.

- In order to help the Awareness subtask obtain a regular, up-to-date overview of the status of security awareness within the European NREN community, two questions about this topic should be added to the GÉANT Compendium questionnaire.
- The Awareness survey should be run on a regular basis (e.g. biannually) to monitor the NRENs' progress and their evolving needs in terms of cyber security awareness.

5.2 Timeline

- November 2023 – October 2024: build, launch and promote the awareness repository on the GÉANT Security website.
- January 2024 – June 2024: start building the awareness community and organise a first meeting/workshop (could be combined with the GÉANT Security Days or TNC24).
- January 2024 – March 2024: identify the relevant contact persons within the NRENs that didn't participate in the awareness survey.
- March 2024 – October 2024: develop new awareness materials for the community and prepare the GÉANT Security Month campaign 2024.
- Next phase of the GN5 Framework Partnership Agreement (FPA) project (starting 2025): develop an awareness game specifically for the NREN community.

Appendix A Overview of NRENs Involved in CSM Campaigns and in the Awareness Survey/Interviews

NREN	Participated at least once in CSM	Participated in the awareness survey	Participated in the interview	Function of the interviewee(s)	Interview date
ACOnet					
AMRES					
ARNES	X	X			
ASNET-AM	X	X			
AzScienceNet					
BASNET					
Belnet	X	X	X	Internal communications officer	03/04/23
BREN					
CARNET	X	X			
CESNET	X	X	X	Security Advisor	06/06/23
CSC/Funet	X	X			
CYNet	X	X	X	Cyber Security Analysts	21/03/23
DeiC	X	X	X	Head of Security, Trust and Identity Services, Information security communications officer	21/04/23

NREN	Participated at least once in CSM	Participated in the awareness survey	Participated in the interview	Function of the interviewee(s)	Interview date
DFN	X	X	X	Corporate communications officer	22/06/23
FCT/FCCN	X				
GARR	X	X	X	Training & e-learning developer	17/05/23
GÉANT	X	X	X	CISO	13/07/23
GRENA	X	X			
GRNET	X	X			
Harno (EEnet)	x				
HEAnet	X	X	X	Technical Services Director	14/04/23
LANET (CERT.LV)	X				
IUCC					
Jisc	X	X			
KIFÜ	X				
KREN					
LITNET	X	X			
MARnet	X				
MREN					
PSNC					
RASH	X	X			
RedIRIS	X	X			
RENAM	X	X			
RENATER	X	X			

NREN	Participated at least once in CSM	Participated in the awareness survey	Participated in the interview	Function of the interviewee(s)	Interview date
RESTENA	X	X	X	CISO	06/04/23
RHnet					
RoEduNet					
SANET					
SUNET	X	X	X	Network and Security services coordinator	21/04/23
Sikt					
SURF	X	X	X	Product Manager Awareness and training, Information Security Officer	05/04/23
SWITCH	X	X	X	Security Awareness Specialist	27/03/23
ULAKBIM		X			
UoM					
URAN					

Appendix B Security Awareness Survey

Security awareness survey

Q1 Your name

Answered: 25 Skipped: 0

Q2 Your role in your organisation

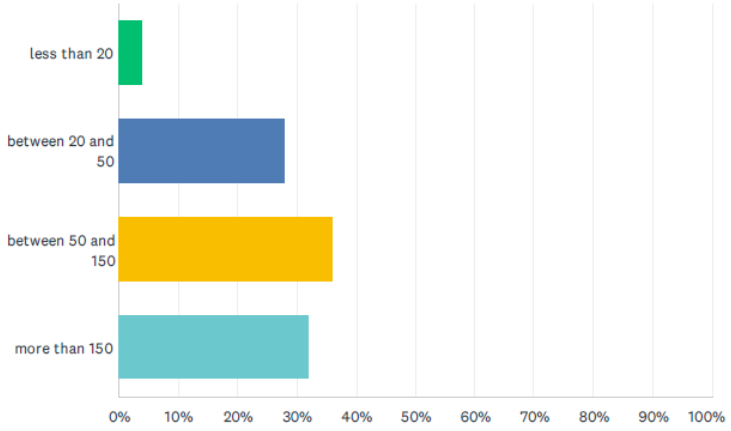
Answered: 25 Skipped: 0

Q3 Name of your NREN

Answered: 25 Skipped: 0

Q4 Number of people working in your NREN

Answered: 25 Skipped: 0

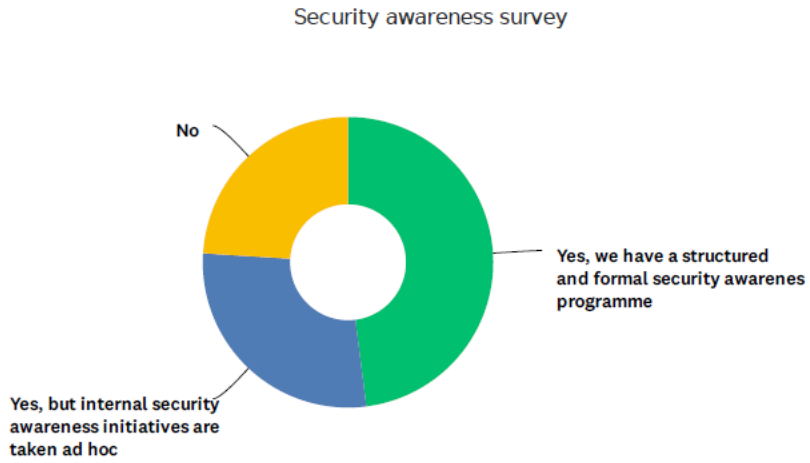


ANSWER CHOICES	RESPONSES	
less than 20	4.00%	1
between 20 and 50	28.00%	7
between 50 and 150	36.00%	9
more than 150	32.00%	8
TOTAL		25

Q5 Does your NREN run an internal security awareness programme?

Answered: 25 Skipped: 0

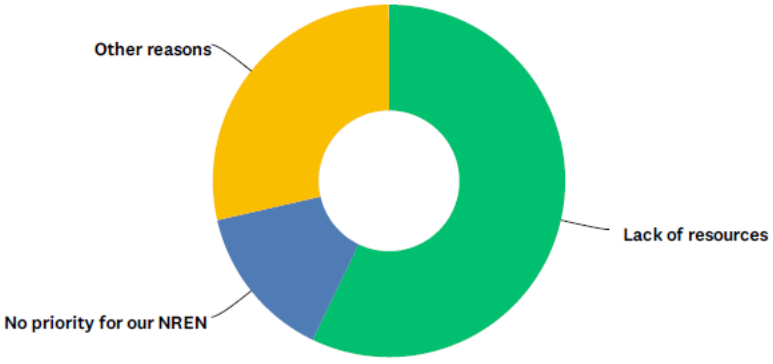
1 / 25



ANSWER CHOICES	RESPONSES	
Yes, we have a structured and formal security awareness programme	48.00%	12
Yes, but internal security awareness initiatives are taken ad hoc	28.00%	7
No	24.00%	6
TOTAL		25

Q6 Why not

Answered: 7 Skipped: 18

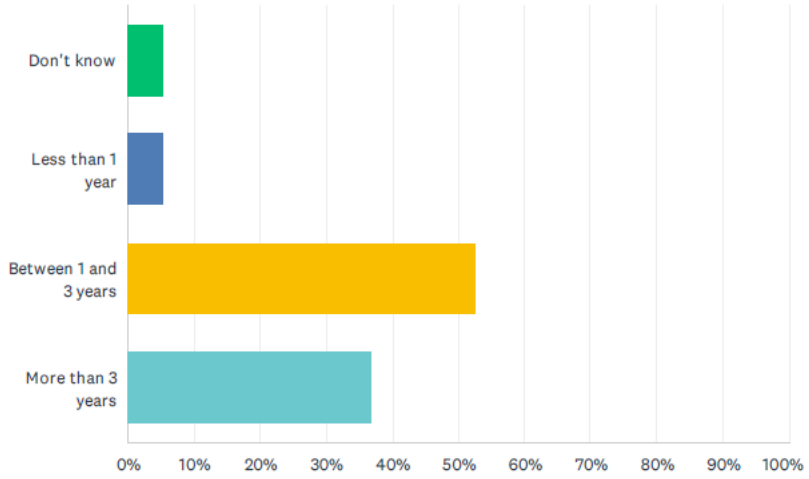


ANSWER CHOICES	RESPONSES	
Lack of resources	57.14%	4
No priority for our NREN	14.29%	1
Other reasons	28.57%	2
TOTAL		7

Security awareness survey

Q7 For how long have you been running an internal awareness programme?

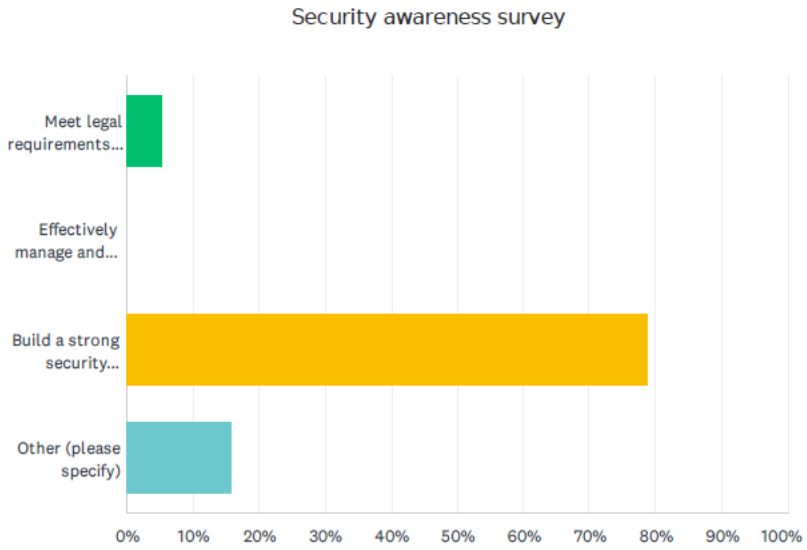
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
Don't know	5.26%	1
Less than 1 year	5.26%	1
Between 1 and 3 years	52.63%	10
More than 3 years	36.84%	7
TOTAL		19

Q8 What is the main purpose of your internal awareness programme?

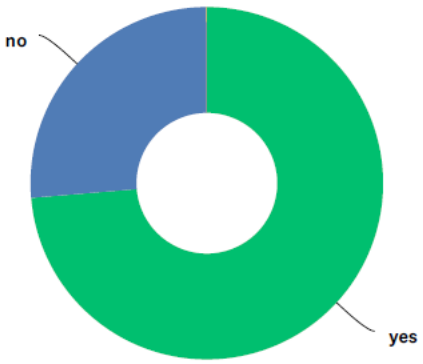
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
Meet legal requirements (compliance / audit)	5.26%	1
Effectively manage and measure human risk	0.00%	0
Build a strong security culture within the organisation	78.95%	15
Other (please specify)	15.79%	3
TOTAL		19

Q9 Have you identified the top human risks in your NREN prior to developing your awareness programme?

Answered: 19 Skipped: 6

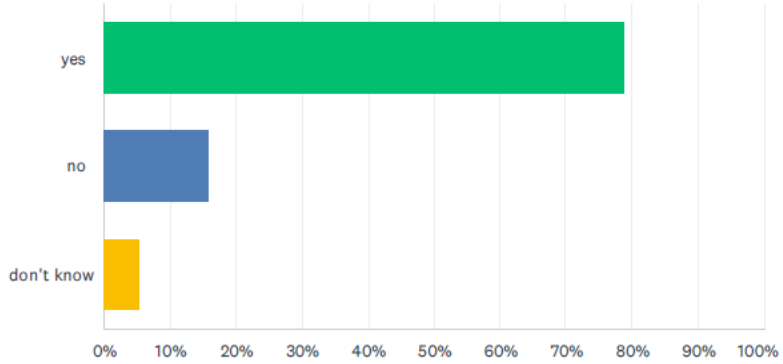


Security awareness survey

ANSWER CHOICES	RESPONSES	
yes	73.68%	14
no	26.32%	5
don't know	0.00%	0
TOTAL		19

Q10 Do you adapt your awareness programme depending on new risks and threats?

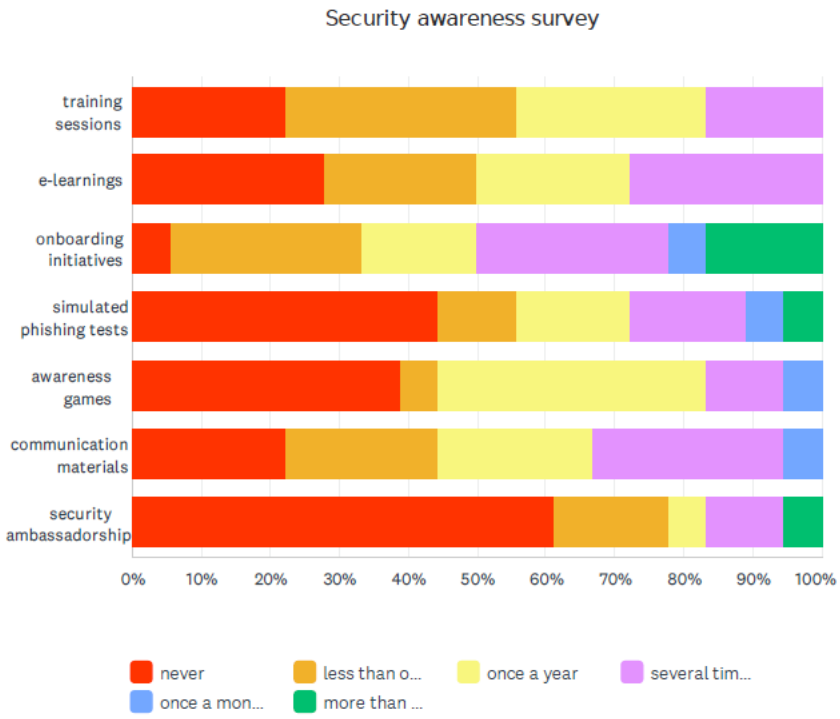
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
yes	78.95%	15
no	15.79%	3
don't know	5.26%	1
TOTAL		19

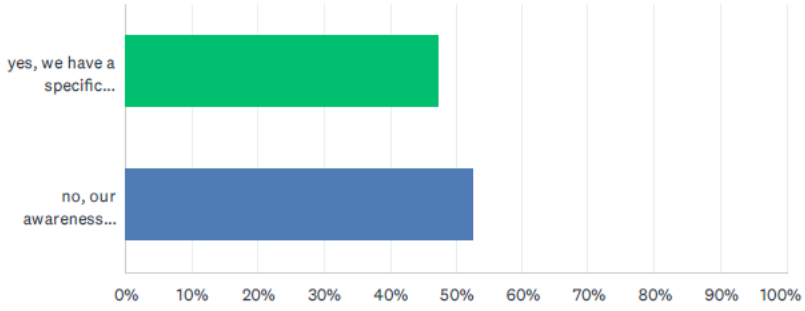
Q11 How frequently do you use the following formats in your internal awareness programme?

Answered: 18 Skipped: 7



Q12 Does your awareness programme make a distinction between different target groups based on specific risks for them (e.g. finance, HR, management, etc)?

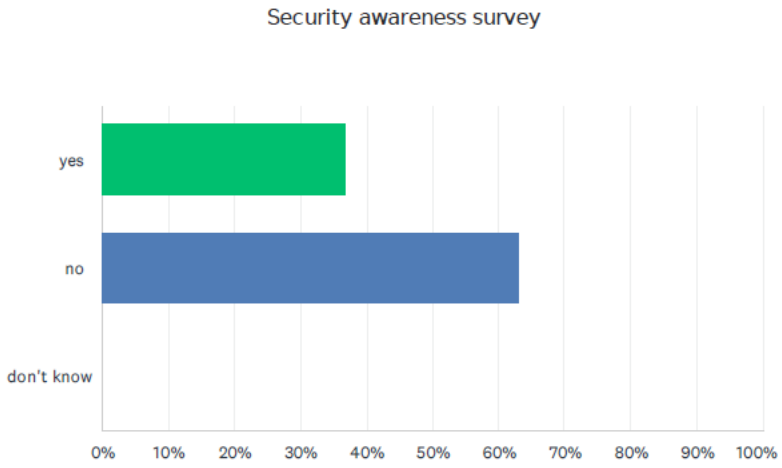
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
yes, we have a specific approach for different target groups	47.37%	9
no, our awareness programme is the same for all employees	52.63%	10
TOTAL		19

Q13 Do you organise specific training for IT and developers?

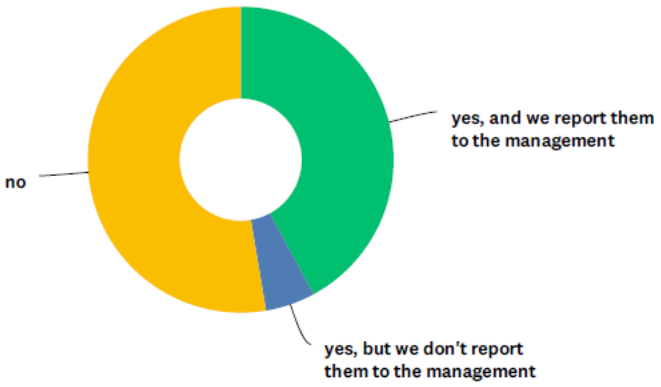
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
yes	36.84%	7
no	63.16%	12
don't know	0.00%	0
TOTAL		19

Q14 Do you use metrics to measure the success of your awareness programme?

Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
yes, and we report them to the management	42.11%	8
yes, but we don't report them to the management	5.26%	1
no	52.63%	10
TOTAL		19

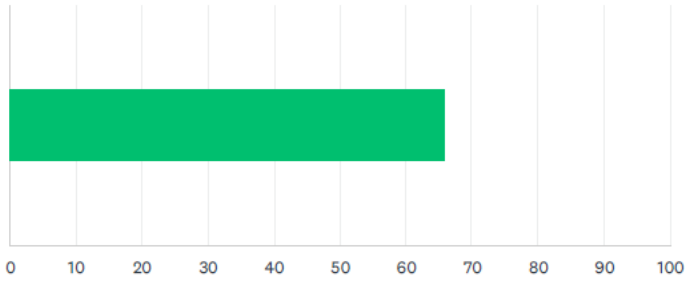
Security awareness survey

Q15 Which metrics do you use?

Answered: 8 Skipped: 17

Q16 In which way is the management of your NREN involved in the security awareness programme?

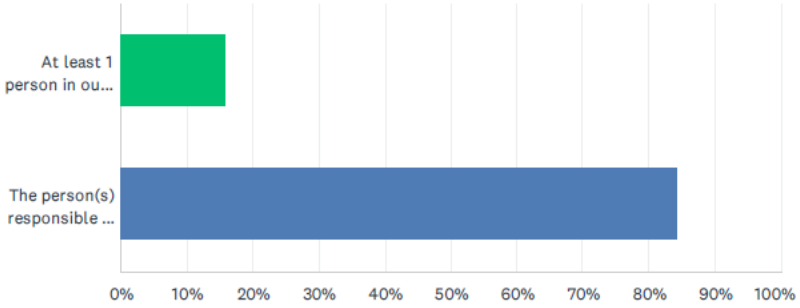
Answered: 19 Skipped: 6



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	66	1,253	19
Total Respondents: 19			

Q17 What resources does your NREN have for internal security awareness?

Answered: 19 Skipped: 6

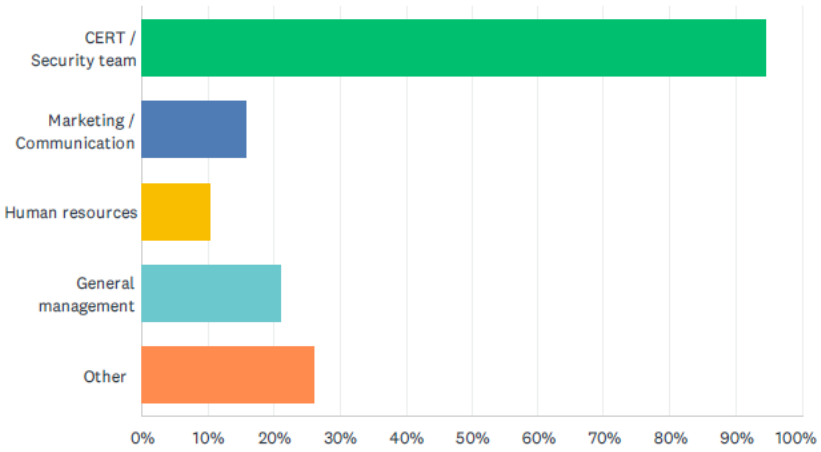


ANSWER CHOICES	RESPONSES	
At least 1 person in our NREN is dedicated full time to internal security awareness	15.79%	3
The person(s) responsible for internal security awareness in our NREN has other (primary) responsibilities	84.21%	16
TOTAL		19

Security awareness survey

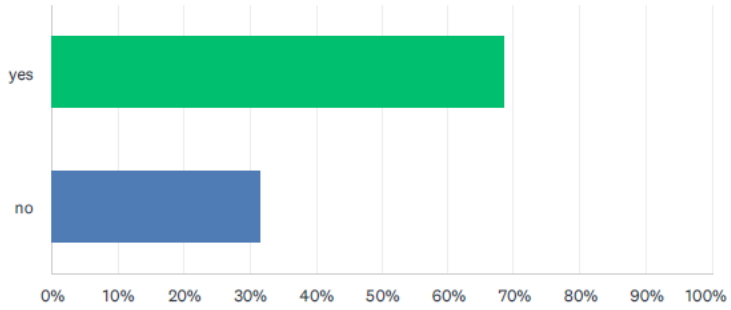
Q18 In which department(s) does this person / do this persons work?

Answered: 19 Skipped: 6



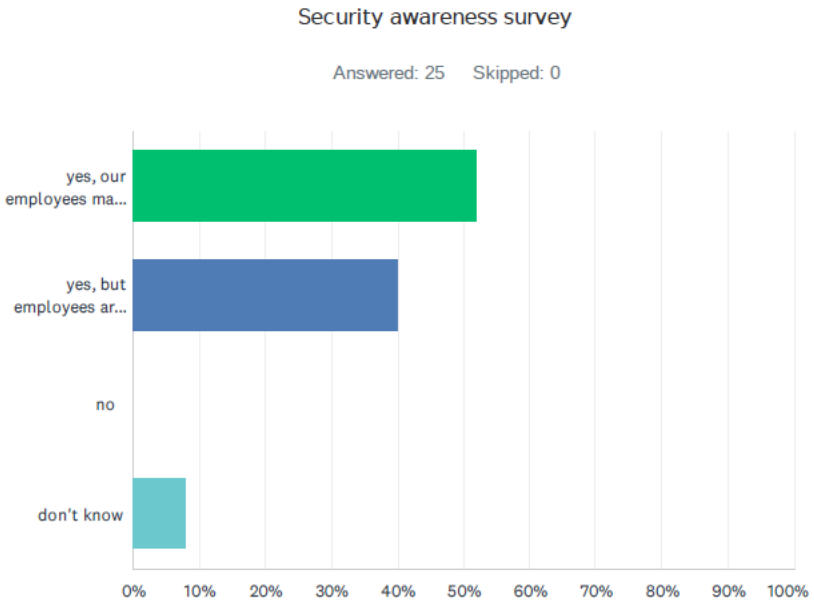
Q19 Does this person coordinate activities with other departments regarding the awareness programme (communication, human resources, IT support, etc)?

Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
yes	68.42%	13
no	31.58%	6
TOTAL		19

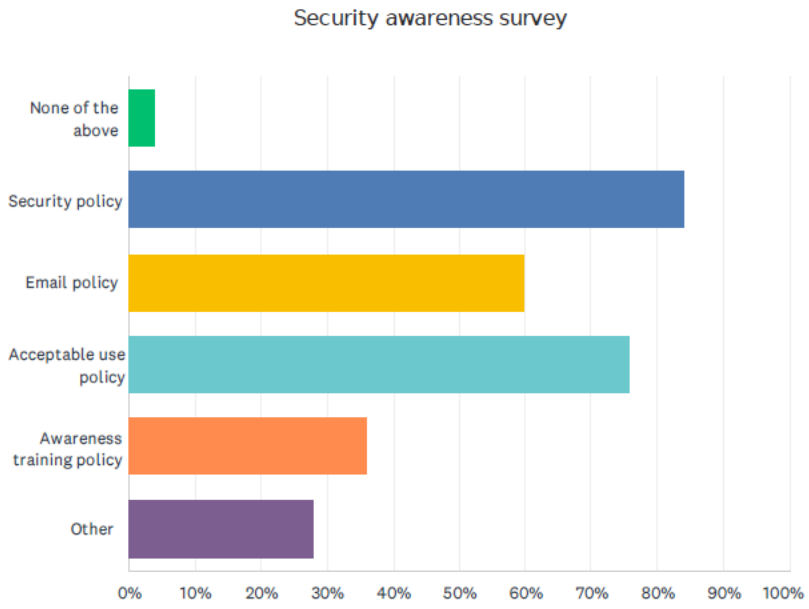
Q20 Do you have an internal procedure to report security incidents?



ANSWER CHOICES	RESPONSES	
yes, our employees make correct use of the procedure	52.00%	13
yes, but employees are insufficiently aware about the procedure	40.00%	10
no	0.00%	0
don't know	8.00%	2
TOTAL		25

Q21 Which security policy/ies exist in your NREN?

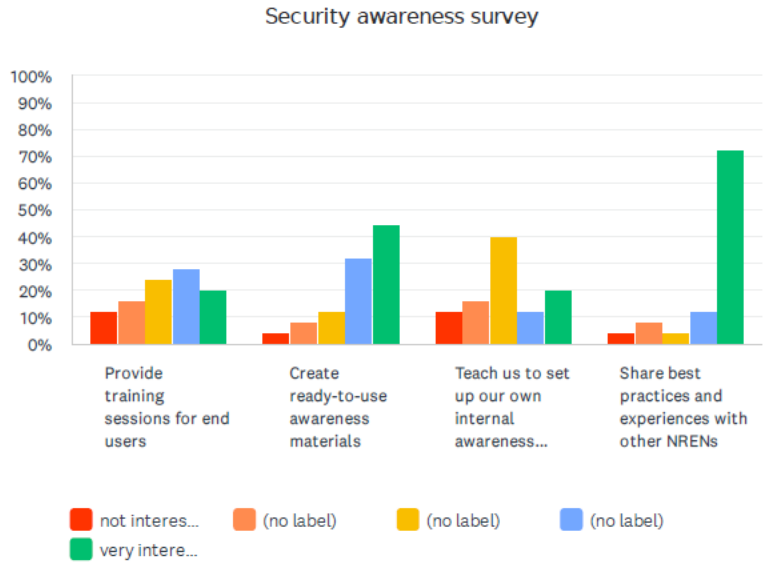
Answered: 25 Skipped: 0



ANSWER CHOICES	RESPONSES	
None of the above	4.00%	1
Security policy	84.00%	21
Email policy	60.00%	15
Acceptable use policy	76.00%	19
Awareness training policy	36.00%	9
Other	28.00%	7
Total Respondents: 25		

Q22 How can GÉANT help you with your internal awareness programme?

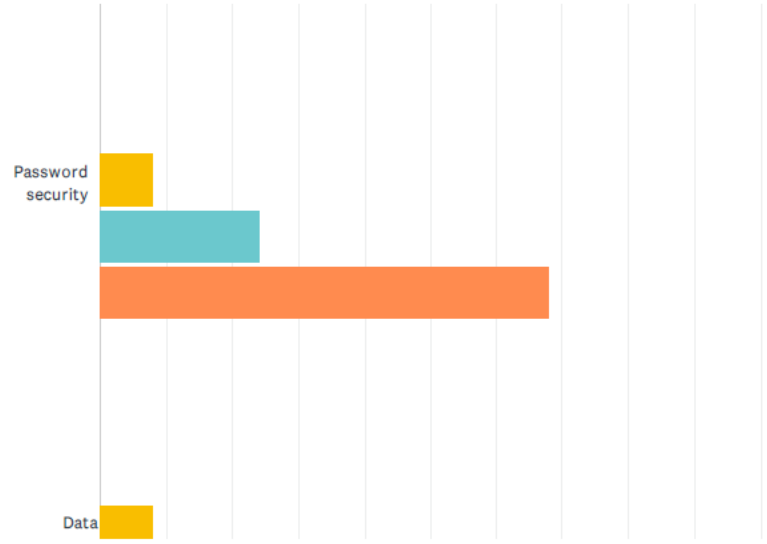
Answered: 25 Skipped: 0



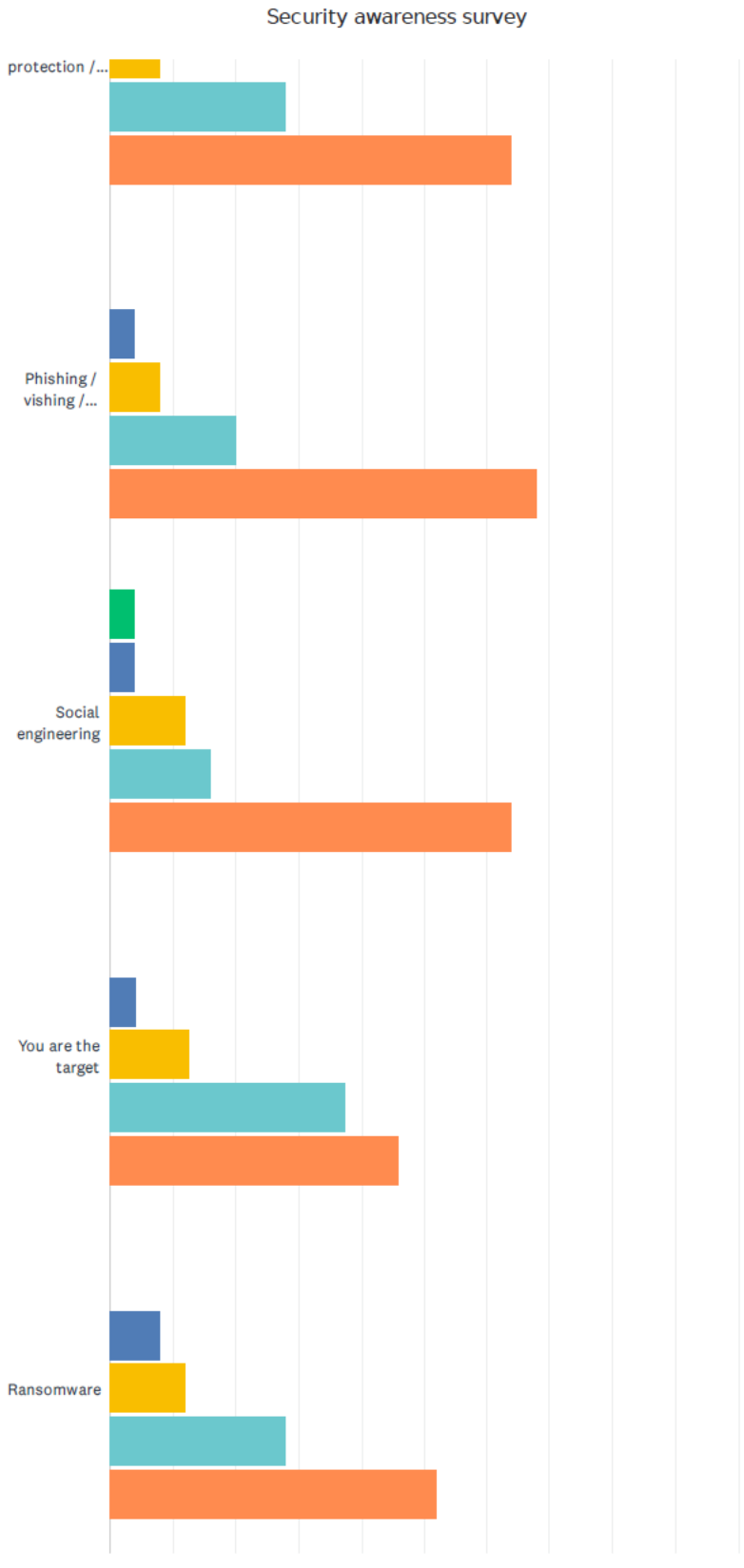
	NOT INTERESTING AT ALL	(NO LABEL)	(NO LABEL)	(NO LABEL)	VERY INTERESTING	TOTAL	WEIGHTED AVERAGE
Provide training sessions for end users	12.00% 3	16.00% 4	24.00% 6	28.00% 7	20.00% 5	25	3.28
Create ready-to-use awareness materials	4.00% 1	8.00% 2	12.00% 3	32.00% 8	44.00% 11	25	4.04
Teach us to set up our own internal awareness programme	12.00% 3	16.00% 4	40.00% 10	12.00% 3	20.00% 5	25	3.12
Share best practices and experiences with other NRENs	4.00% 1	8.00% 2	4.00% 1	12.00% 3	72.00% 18	25	4.40

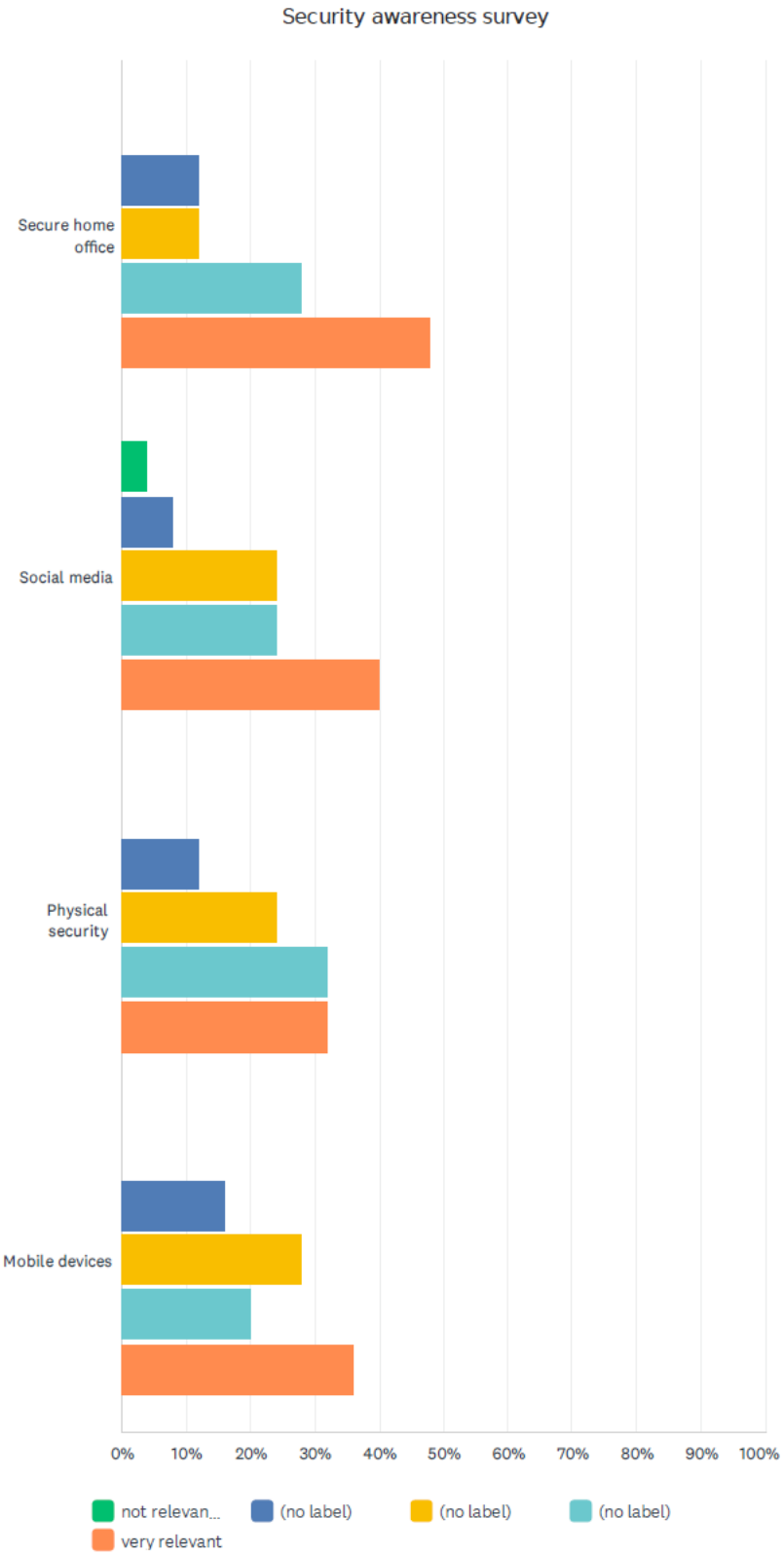
Q23 Which topics do you consider most relevant for your NRENs internal security awareness programme?

Answered: 25 Skipped: 0



12 / 25


Security awareness survey
protection /...
Phishing / vishing /...
Social engineering
You are the target
Ransomware
13 / 25


Security awareness survey
Secure home office
Social media
Physical security
Mobile devices
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
not relevan...
(no label)
(no label)
(no label)
very relevant

14 / 25

Security awareness survey

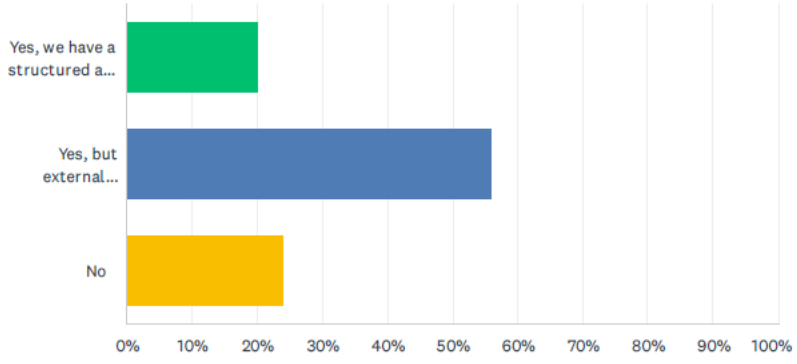
	NOT RELEVANT AT ALL	(NO LABEL)	(NO LABEL)	(NO LABEL)	VERY RELEVANT	TOTAL	WEIGHTED AVERAGE
Password security	0.00% 0	0.00% 0	8.00% 2	24.00% 6	68.00% 17	25	4.60
Data protection / privacy	0.00% 0	0.00% 0	8.00% 2	28.00% 7	64.00% 16	25	4.56
Phishing / vishing / smishing	0.00% 0	4.00% 1	8.00% 2	20.00% 5	68.00% 17	25	4.52
Social engineering	4.00% 1	4.00% 1	12.00% 3	16.00% 4	64.00% 16	25	4.32
You are the target	0.00% 0	4.17% 1	12.50% 3	37.50% 9	45.83% 11	24	4.25
Ransomware	0.00% 0	8.00% 2	12.00% 3	28.00% 7	52.00% 13	25	4.24
Secure home office	0.00% 0	12.00% 3	12.00% 3	28.00% 7	48.00% 12	25	4.12
Social media	4.00% 1	8.00% 2	24.00% 6	24.00% 6	40.00% 10	25	3.88
Physical security	0.00% 0	12.00% 3	24.00% 6	32.00% 8	32.00% 8	25	3.84
Mobile devices	0.00% 0	16.00% 4	28.00% 7	20.00% 5	36.00% 9	25	3.76

Q24 Number of end users in your NREN member organisations (estimation)

Answered: 22 Skipped: 3

Q25 Does your NREN run an external awareness programme?

Answered: 25 Skipped: 0

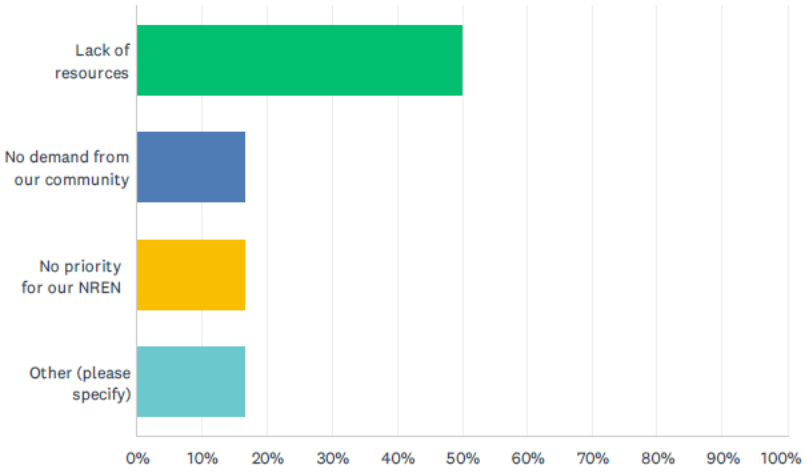


Security awareness survey

ANSWER CHOICES	RESPONSES	
Yes, we have a structured and formal awareness programme	20.00%	5
Yes, but external awareness initiatives are taken ad hoc	56.00%	14
No	24.00%	6
TOTAL		25

Q26 Why not?

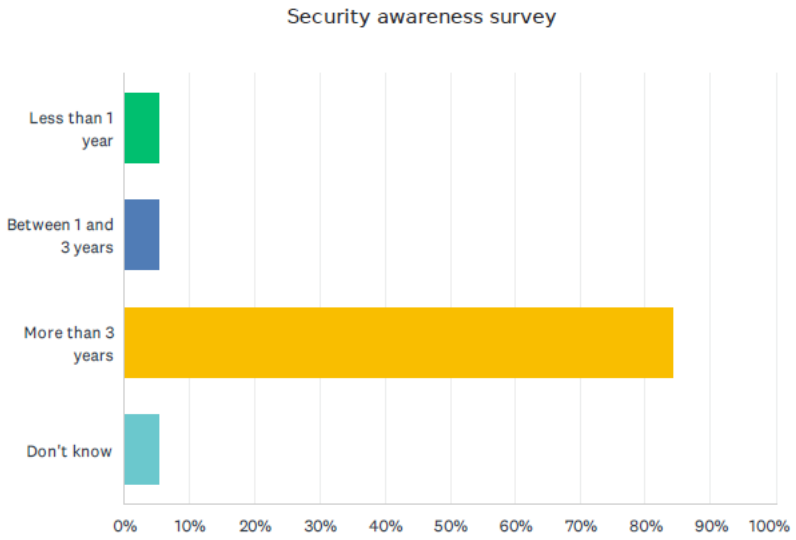
Answered: 6 Skipped: 19



ANSWER CHOICES	RESPONSES	
Lack of resources	50.00%	3
No demand from our community	16.67%	1
No priority for our NREN	16.67%	1
Other (please specify)	16.67%	1
TOTAL		6

Q27 For how long have you been running an external awareness programme?

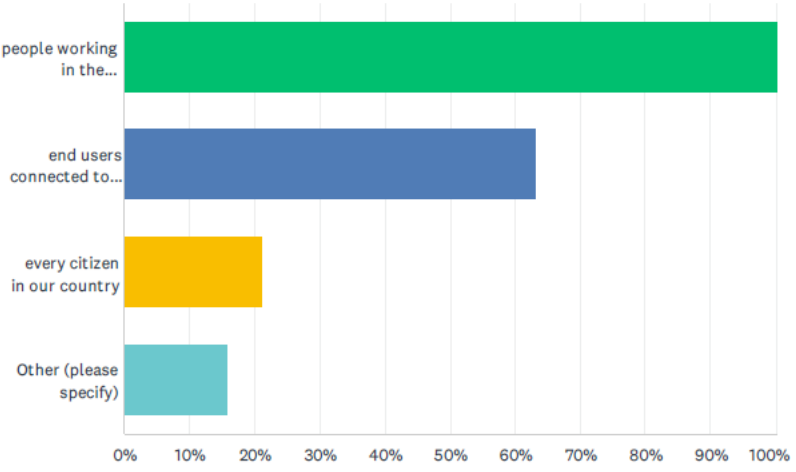
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
Less than 1 year	5.26%	1
Between 1 and 3 years	5.26%	1
More than 3 years	84.21%	16
Don't know	5.26%	1
TOTAL		19

Q28 Who is your target audience (several answers possible)?

Answered: 19 Skipped: 6

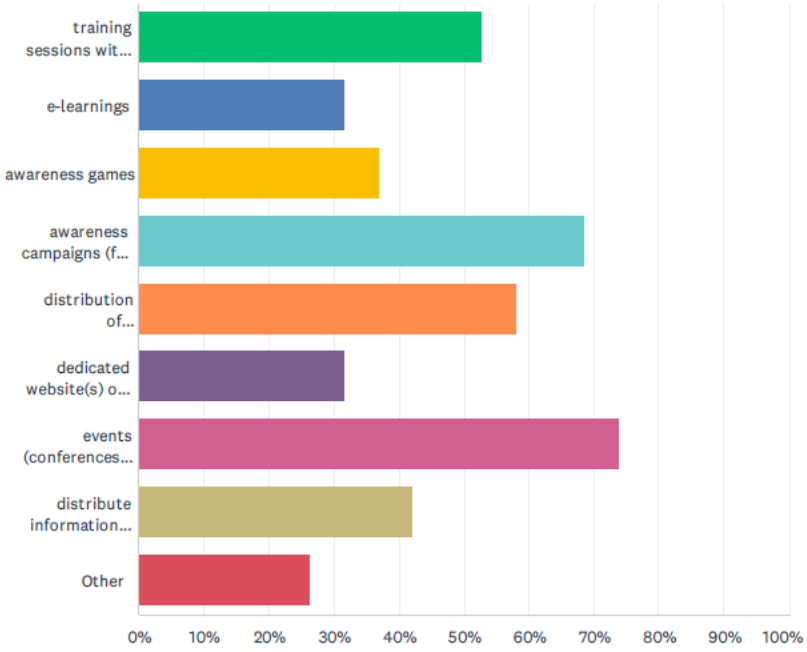


Security awareness survey

ANSWER CHOICES	RESPONSES	
people working in the organisations connected to our NREN	100.00%	19
end users connected to our NREN (students, reseachers, ...)	63.16%	12
every citizen in our country	21.05%	4
Other (please specify)	15.79%	3
Total Respondents: 19		

Q29 In what consists your external awareness programme?

Answered: 19 Skipped: 6

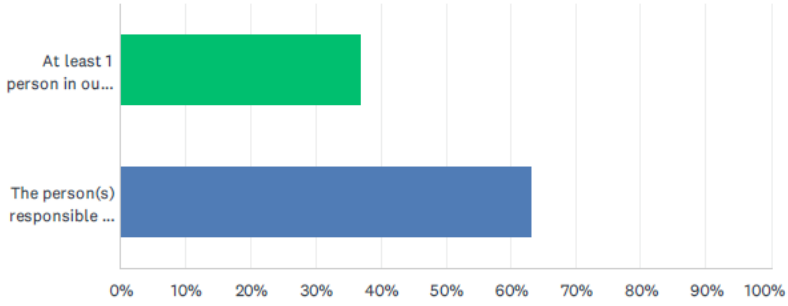


Security awareness survey

ANSWER CHOICES	RESPONSES	
training sessions with instructor	52.63%	10
e-learnings	31.58%	6
awareness games	36.84%	7
awareness campaigns (for example during the European Cyber Security Month)	68.42%	13
distribution of communication materials (posters, flyers, videos ...)	57.89%	11
dedicated website(s) on security awareness	31.58%	6
events (conferences or workshops)	73.68%	14
distribute information about existing awareness initiatives and tools from other organisations	42.11%	8
Other	26.32%	5
Total Respondents: 19		

Q30 What resources does your NREN have for external security awareness?

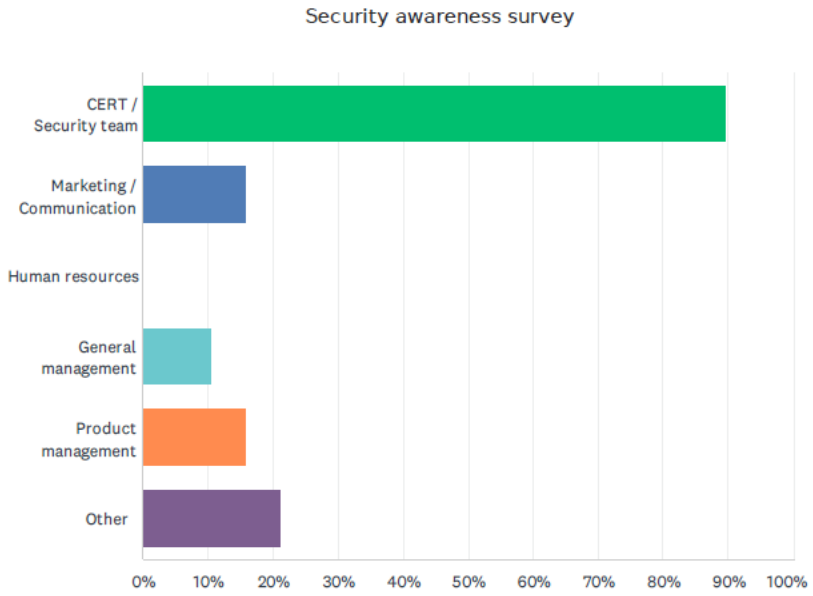
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
At least 1 person in our NREN is dedicated full time to external security awareness	36.84%	7
The person(s) responsible for external security awareness in our NREN has other (primary) responsibilities	63.16%	12
TOTAL		19

Q31 In which department does this person / do these persons work?

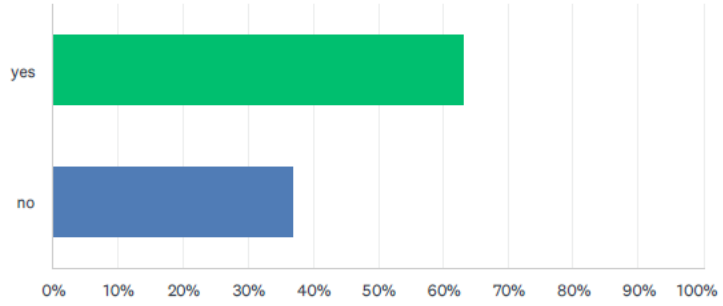
Answered: 19 Skipped: 6



ANSWER CHOICES	RESPONSES	
CERT / Security team	89.47%	17
Marketing / Communication	15.79%	3
Human resources	0.00%	0
General management	10.53%	2
Product management	15.79%	3
Other	21.05%	4
Total Respondents: 19		

Q32 Does this person coordinate activities with other departments regarding the external awareness programme (communication, human resources, IT support, etc)?

Answered: 19 Skipped: 6

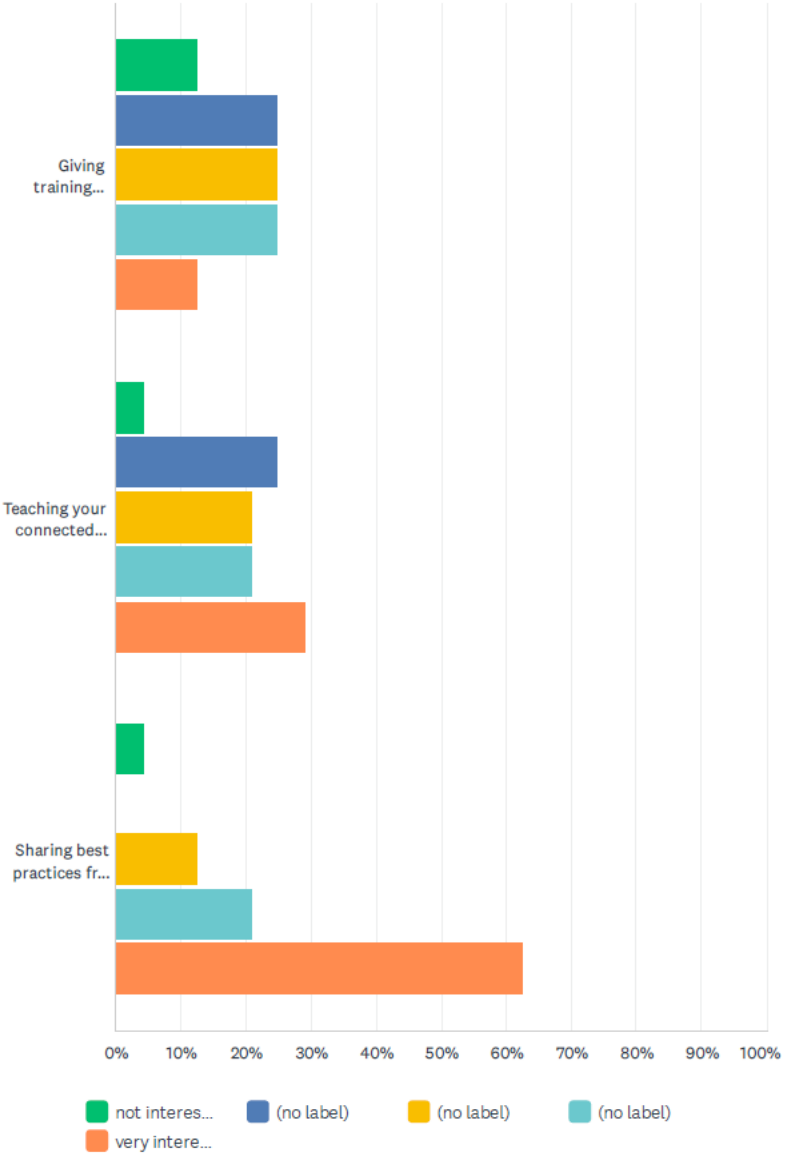


Security awareness survey

ANSWER CHOICES	RESPONSES	
yes	63.16%	12
no	36.84%	7
TOTAL		19

Q33 How can GÉANT help you with your external awareness programme?

Answered: 24 Skipped: 1



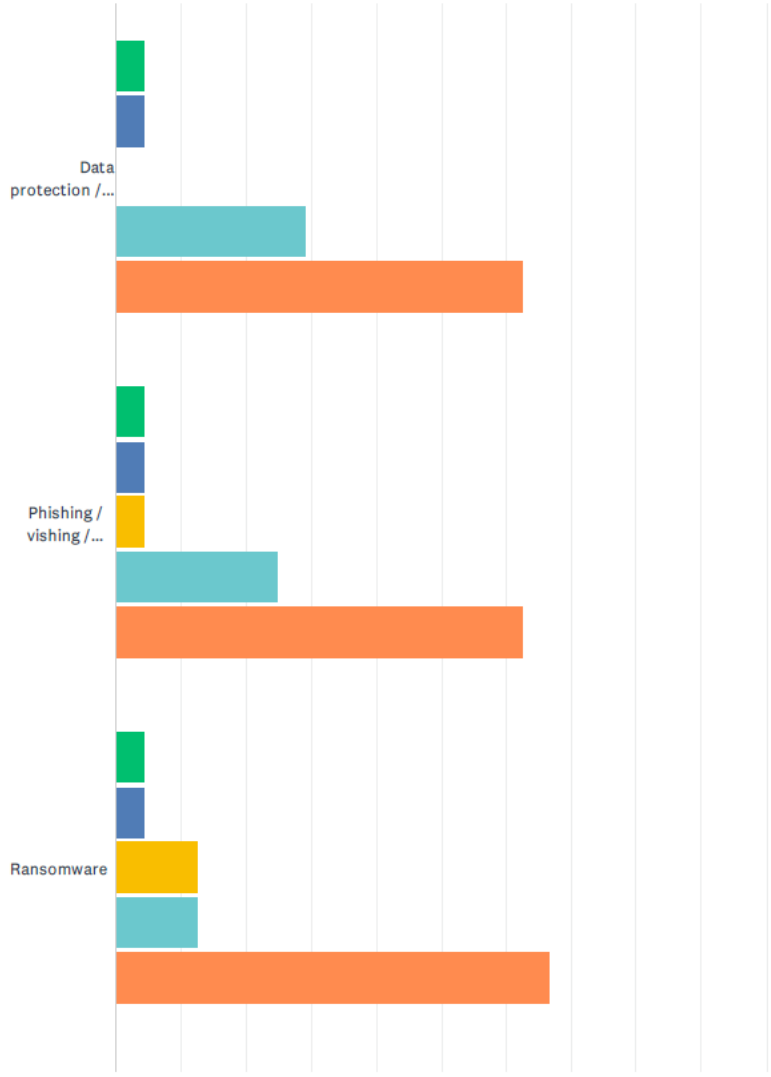
21 / 25

Security awareness survey

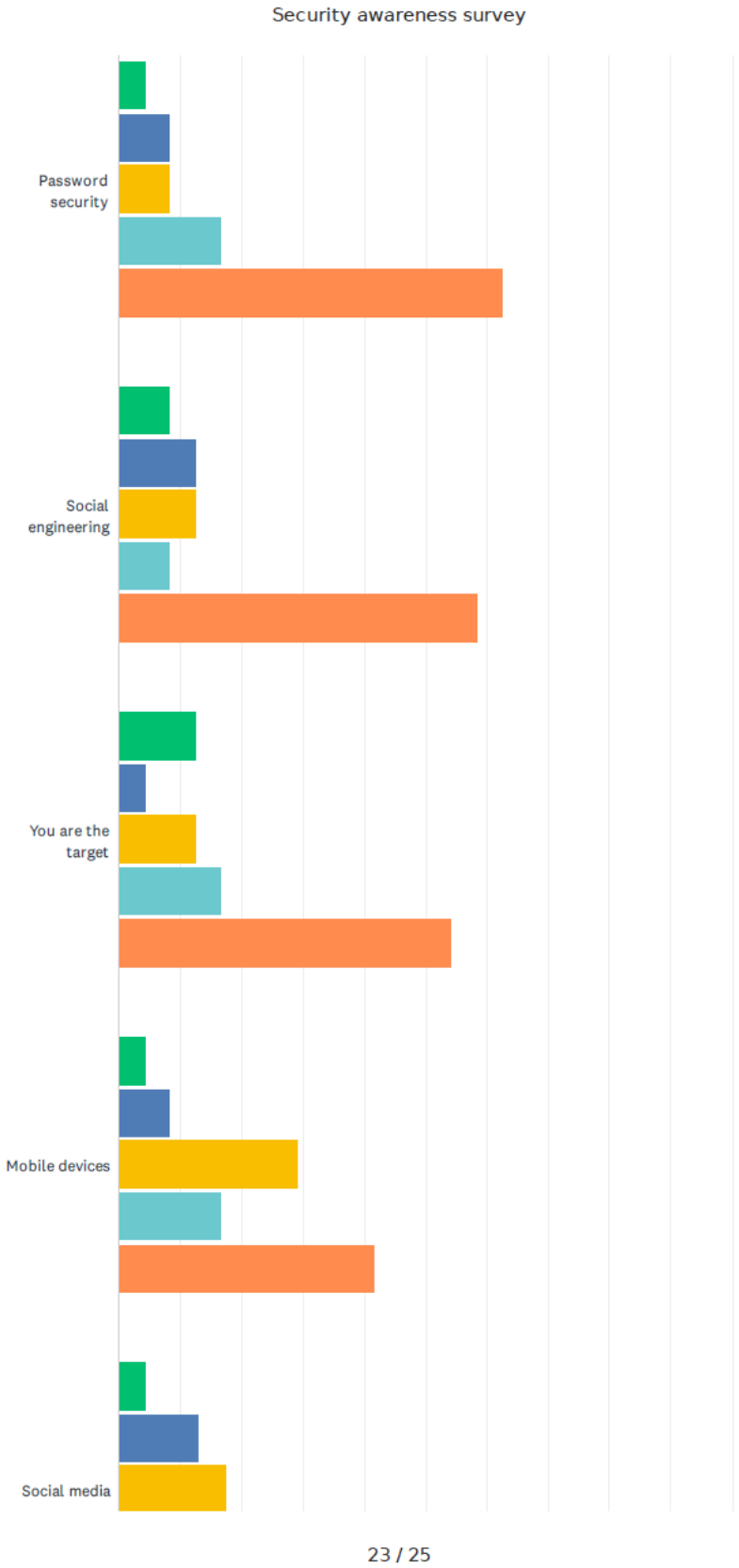
	NOT INTERESTING AT ALL	(NO LABEL)	(NO LABEL)	(NO LABEL)	VERY INTERESTING	TOTAL	WEIGHTED AVERAGE
Giving training sessions for end users	12.50% 3	25.00% 6	25.00% 6	25.00% 6	12.50% 3	24	3.00
Teaching your connected organisations how to set up their own awareness programme	4.17% 1	25.00% 6	20.83% 5	20.83% 5	29.17% 7	24	3.46
Sharing best practices from the GÉANT community	4.17% 1	0.00% 0	12.50% 3	20.83% 5	62.50% 15	24	4.38

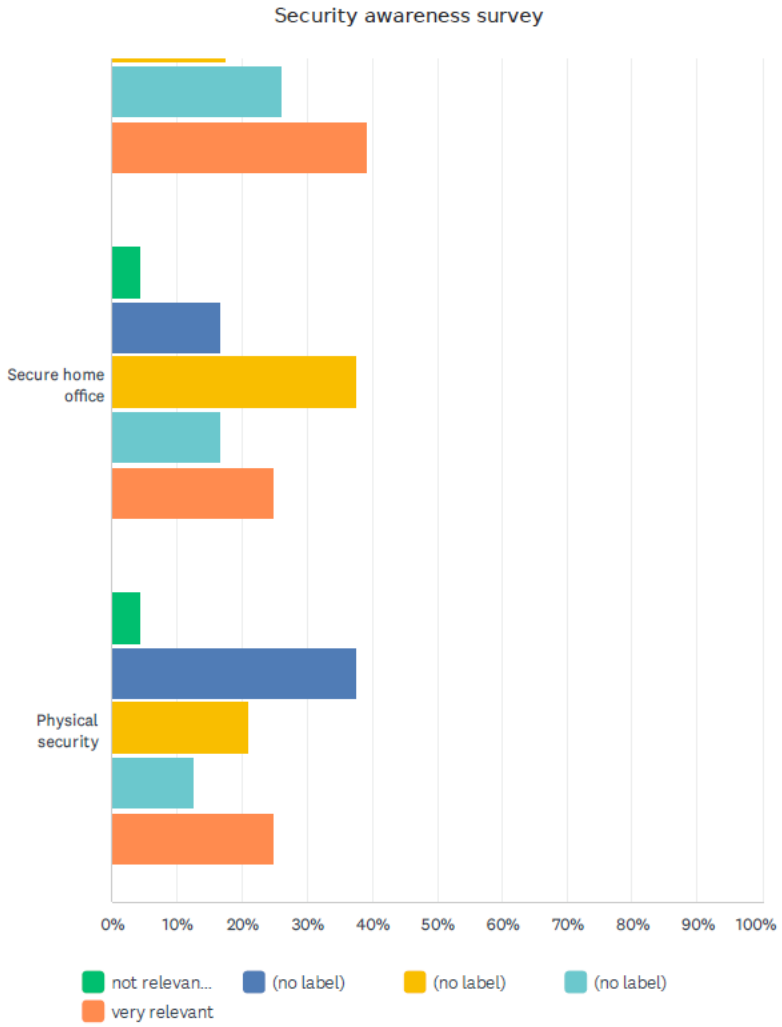
Q34 Which topics do you consider most relevant for your NRENs external security awareness programme?

Answered: 24 Skipped: 1



22 / 25


Security awareness survey
Password security
Social engineering
You are the target
Mobile devices
Social media
23 / 25


Security awareness survey
Secure home office
Physical security
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
not relevan...
(no label)
(no label)
(no label)
very relevant

Security awareness survey

	NOT RELEVANT AT ALL	(NO LABEL)	(NO LABEL)	(NO LABEL)	VERY RELEVANT	TOTAL	WEIGHTED AVERAGE
Data protection / privacy	4.17% 1	4.17% 1	0.00% 0	29.17% 7	62.50% 15	24	4.42
Phishing / vishing / smishing	4.17% 1	4.17% 1	4.17% 1	25.00% 6	62.50% 15	24	4.38
Ransomware	4.17% 1	4.17% 1	12.50% 3	12.50% 3	66.67% 16	24	4.33
Password security	4.17% 1	8.33% 2	8.33% 2	16.67% 4	62.50% 15	24	4.25
Social engineering	8.33% 2	12.50% 3	12.50% 3	8.33% 2	58.33% 14	24	3.96
You are the target	12.50% 3	4.17% 1	12.50% 3	16.67% 4	54.17% 13	24	3.96
Mobile devices	4.17% 1	8.33% 2	29.17% 7	16.67% 4	41.67% 10	24	3.83
Social media	4.35% 1	13.04% 3	17.39% 4	26.09% 6	39.13% 9	23	3.83
Secure home office	4.17% 1	16.67% 4	37.50% 9	16.67% 4	25.00% 6	24	3.42
Physical security	4.17% 1	37.50% 9	20.83% 5	12.50% 3	25.00% 6	24	3.17

References

[CSM] https://connect.geant.org/cyber-security-month
[SANS] https://www.sans.org/security-awareness-training/resources/maturity-model/
[ISO27001] https://www.iso.org/standard/27001

Glossary

BCP	Business Continuity Plan
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSM	Cyber Security Month
FPA	Framework Partnership Agreement
FTE	Full-Time Equivalent
GN4-3	GÉANT Network 4 Phase 3, a project part-funded by the EC's Horizon 2020 programme under Specific Grant Agreement No. 856726
GN5-1	GÉANT Network 5, Phase 1, a project funded by the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101100680 and one of the projects implementing the actions defined in the GN5-FPA
HR	Human Resources
ISMS	Information Security Management System
NREN	National Research and Education Network
QR code	Quick-response code
SANS	SysAdmin, Audit, Network, and Security
T	Task
TNC	The Networking Conference, the largest and most prestigious research and education networking conference, and GÉANT's flagship event
WP	Work Package