13-04-2018

# White Paper: Security and Privacy

Authors: Alf Moens (SURFnet), Sigita Jurkynaitė (GÉANT Association)


The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2)

# Contents

# 1 Background and Introduction

In its most recent publication on cybersecurity, the European Commission recognises it as 'critical to both our prosperity and our security' [EC-JOIN-450]. The EC proceeds to emphasise the importance of cybersecurity by explaining that '[as] our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats […]'.

The NRENs are facing the same security challenges, both individually and as a community – the functioning of their infrastructures, be it the network or other infrastructural services, depends heavily on cybersecurity readiness. Currently, many NRENs still have a long way to go to gain control of security and privacy in order to keep delivering trustworthy services for research and education communities in their constituencies and beyond. GÉANT, as Europe's leading collaboration on e-infrastructure and services for research and education, must take a very active role in 'guaranteeing privacy through policy and technology and ensuring the robustness and trustworthiness of systems by continuous security improvements', as noted in *GÉANT Strategy 2020* [GÉANT-Strat2020].

This white paper aims to provide guidance for security and privacy activities for GÉANT and the NRENs for the period of 2019 to 2022. It addresses some of the cybersecurity challenges of the NREN community, focusing on six main areas (in no particular order of priority):

- Security baselining for products, services and organisations.
- Managed security products and services.
- Legal and privacy compliance.
- Management of risks.
- Training and awareness.
- Incident response, business continuity and crisis management.

The subject areas are not independent, they are related and influence each other. The results of one area will be of high importance for another. These interdependencies will need to be identified and detailed in any future work. Also, the work in some subjects might result in new products and services. The authors have chosen to group subjects together in main subject areas, and not according to potential for service development.

This white paper is targeted at a broad audience from both GÉANT and the NRENs, and from both decision-making and security and privacy management, and technical security operations and security and privacy product development. A large number of the subjects will also be of interest for the constituents of the NRENs.

## 1.1 Method

In preparation for writing the white paper, four public community consultations were held (virtual and face to face), which were open to everyone to attend. In total, there were 60 participants from 27

organisations (NRENs, infrastructures and universities). During the consultations, participants were asked to provide feedback on the main areas identified, comment on what is already being done and suggest new, innovative ideas for security- and privacy-related activities. After that, attendees were invited to rate the suggestions based on their relevance, to find out which are the most urgent ideas that should be implemented in the four years of GN4-3.[1] The input collected was used in writing this white paper.

To further expand the community involvement, a draft of the white paper was shared with the volunteer reviewers – security experts from Europe [Reviewers] and senior security experts from Internet2, REANNZ, and other organisations outside of the EU.

## 1.2 Security Communities

It is important to mention that all of the discussions in preparation for writing the white paper were held with the existing collaborations in the security and privacy area in mind. As a result of growing interest in this area, several new international initiatives have been launched recently for working together to address security challenges faced by NRENs and e-infrastructures, in addition to groups that have already been working together for years.

The Task Force on Computer Security Incident Response Teams (TF-CSIRT) (running since 2000) and the Special Interest Group on Information Security Management (SIG-ISM) (established in 2014) are part of GN4-2 NA3 T5. Various other R&E security working groups [SecGroups] are supported by the Community Support Office (CSO) team within GÉANT, both within the GÉANT realm and globally with the WISE community (e-infrastructures) and the Global NREN Security Group. Through this shared management support and through shared memberships, the communities fine-tune their agendas and exchange results.

During the consultations, the community continually expressed the need for collaboration, information and best-practice sharing. Therefore it is crucial that those groups continue to exist and grow, supported by GÉANT, as they are essential to the process of information sharing and working together on all of the strategic topics. However, there is scope to improve information sharing about who is working on what, the status of the work, and processes that are already established and still missing. Joint info-share sessions on the groups and presentations to the community would be a good way of keeping everyone informed and of getting new colleagues involved.

# 2 Security Baselining for Products, Services and Organisations

**Main goal**: provide means for implementing security controls and security management in order to justify mutual trust, and compliance with rules and regulations.

Security can be arranged in a large number of ways. In order to be able to verify mutual trust and cooperate in a safe and secure fashion, the use of standards for security and privacy is recommended. There are international standards, technical and organisational bodies, such as ETSI, IWGDPT, ENISA, ISO 27001, NIST and others, that should be used as a base, complete with standards and guidelines

[1] The results and notes of the consultation sessions can be found at [GN4-3_SecPlanning].

for implementation and measuring compliance. A periodic benchmark, describing maturity and compliance, can help enforce trust and help point out areas where the organisation has moved forward as well as areas where the organisation is falling behind and needs to improve.

Several groups in research and education have already put security frameworks into practice:

- Norwegian HE (UNINETT): based on ISO 27001.
- Dutch HE (SURFnet): Dutch HE security framework based on ISO 27000.
- WISE, e-infrastructures: SCI framework.
- German HE (DFN): certified baseline protection based on ISO2700x.
- TF-CSIRT: accreditation and certification based on SIM3 of CERTs/CSIRTs and other security entities.
- REFEDS: Sirtfi framework.
- Technical baselines based on NIST.

Some of these frameworks cover only specific processes, such as incident response and user management; other frameworks cover all security aspects.

With this subject area, the aim is not security certification or preparation for certification; instead the aim is to bring security under control, prove mutual trust, and identify and share good practices.

## 2.1 Planned Benefits and Impacts to the User Community

There are large differences between NRENs concerning the processes and facilities for security. Some NRENs have formalised processes and are certified, for parts of their operation, for the security standard ISO 27001. The driver for certification may be external pressure, or may be internal motivation such as demonstrating publicly the compliance with privacy regulations to support the adoption of services that have a huge impact on privacy concerns.

Other NRENs feel neither an internal nor external need for certification and are just looking for the most efficient way to bring security under control. Sharing technical baselines – for example, for hardening servers and other equipment – will assist NRENs and help them verify or implement security controls.

With the selection of a basic set of standards and by sharing good practices, NRENs (and constituents) can make a quick start with implementing and improving security and privacy practices. Using a benchmarking system, for self-assessments or peer reviews, NRENs can determine what level of security is 'fit for purpose' or 'best of breed', whichever meets the needs of the NREN. The benchmarking system can show and enforce the minimal set of security controls that are essential for proving mutual trust.

No matter which standards are chosen, addressing security and privacy is a continuous process that needs to be managed. Security management, whether as part of or as the start of total quality management, enforces continuous attention to implementing and improving security and privacy. Through a regular annual planning and control cycle, security and privacy can be managed and improved in an organised manner with a clear view of anticipated results and the resources needed for achieving these results.

Though the main target group of this subject area is the NREN, the same will apply and is suitable for the constituents of the NREN.

## 2.2 Implementation

A number of NRENs already have a lot of experience with technical baselining, setting up security management and preparing for certification. Other NRENs are much more involved with their constituents and have set up baselines, reference frameworks and model policies for them. The activities in this subject area will bring these experiences together to identify what is missing and set up a coherent set of baselines, both technical and organisational; agree upon frameworks; and set up and test a benchmarking system based upon these frameworks.

A summary of the proposed key performance indicators for this subject area over the GN4-3 period is given in Table 2.1 below.

| Area of Activity | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| Technical baselines | Develop 2 baselines | Develop 2 baselines | Develop 2 baselines | Develop 2 baselines |
| Security baselines | Reference framework | Develop 2 good practices | Develop 2 good practices | Develop 2 good practices |
| Security management | Select security management framework | Implement security management at 2 NRENs | Implement security management at 2 NRENs | Implement security management at 2 NRENs |
| Benchmarking | Reference framework | Test benchmark group | Annual benchmark | Annual benchmark |
| International standards engagement | Monitor and engage with standards development | Monitor and engage with standards development | Monitor and engage with standards development | Monitor and engage with standards development |

Table 2.1: Summary of proposed baselining KPIs over GN4-3

Topics may include (suggested by the community):

- Standards and baselines for NRENs, information security management system.
- Implementation and evaluation guidance.
- Baselining and benchmarking system with maturity and/or trust model.
- Baselining and benchmarking system including security assessments for constituents.
- Engagement with international standards development.

# 3 Managed Security Products and Services

**Main goal**: develop and manage services delivered by NRENs or joint services delivered by GÉANT, and research the use of emerging technologies.

GÉANT and the NRENs have a rich history of developing successful security products and services that can count on a broad acceptance and usage. Certificate services, security portals, Distributed Denial of Service (DDoS) detection and Firewall on Demand are excellent examples. Recently, new demands have arisen as the number and volume of threats to the infrastructures have increased. For example, the amount of available data about attacks is too large to be handled manually, therefore automation is really needed, while at the same time even better detection capabilities need to be developed.

The plan for this area of work is to continue development of existing solutions and start working on new tools and services. Different groups and stakeholders within the research community (WISE, Sirtfi, CERTs, etc.) are working on these or similar tasks currently. Integration and coordination of these efforts should be an integral part of all the activities outlined in this white paper.

Due to the long planning period, and based on long-term experience, the plan must take into account that there will be as yet unknown demand for additional solutions, tools and services. Some of these needs might be related to new, upcoming serious threats, therefore they might need to be given a higher priority or require new approaches to existing solutions and/or services.

Solutions and services that shall be developed and further improved are:

- Firewall on Demand (FoD).
- Centralised DDoS mitigation.
- Security operations centre (SOC) operations and tools.
- Vulnerability assessment 'as a service'.
- eduVPN.

Each of these is described below.

## 3.1 Firewall on Demand (FoD)

The Firewall on Demand (FoD) service has been a huge success and has provided cutting-edge firewalling that is unavailable to almost any other internet customer. Several improvements and additions are needed to meet the growing demand from the user point of view. Suggestions from the community consultations include:

- Generalised multi-domain Firewall on Demand interface supporting FlowSpec and, if necessary, additional protocols.
- Firewall on Demand as multi-domain interface to allow integration into the coordinated DDoS mitigation across multiple domains (GÉANT, NRENs, institutions).
- QWeb application firewall functions.
- Delivery of attack and monitoring data to improve analysis by CERTs and SOC.

## 3.2 Centralised DDoS Mitigation

Distributed Denial of Service (DDoS) is a growing problem in the R&E community's networks. Several NRENs already have a solution in place for detecting and mitigating DDoS and DoS attacks, but none is ideal and few are comprehensive. A centralised solution needs to be investigated.

For detection, several flow-analysis solutions are used, but none of them is ideal.

Mitigation usually involves a mix of semi-automated steps but depends in many cases on NOC members to manually configure or adjust the existing toolset.

What is missing is a coordinated approach, to mitigate attacks affecting multiple services and/or NRENs. In this work area, experience and expertise will be combined to build a dedicated, fit-for-purpose flow-analysis tool, share good practices, and investigate possible approaches to identify and develop centralised and decentralised detection and mitigation solutions for either centralised or community-oriented coordination in case of attacks.

This will enable the NRENs not only to mitigate DDoS on the network level, but also to provide constituent-focused services to address DDoS attacks that impair not the NREN's infrastructure but the organisation connected to the NREN network. As this might require local detection mechanisms that communicate with any NREN-level detection mechanism, and most likely will involve cross-NREN alerting mechanisms as well, the ability to provide suitable protection on the levels of GÉANT, NREN, constituent and maybe even server will become possible and deployable.

## 3.3 Security Operations Centre Operations and Tools

Security operations consist of a large set of activities and tools that allow security teams – either dedicated Security Operations Centre (SOC) or Computer Emergency Response Team (CERT) teams or a two-tier approach combining SOC and CERT – to identify potential security incidents and address occurring attacks by applying default security controls, without the need for much analysis, based on well-understood use cases and attack-patterns. Some of the tools, use cases and processes are easy to share. Some will require training and documentation to adopt the available solutions in different operational infrastructures. Either way there is a need to operate jointly in the case of shared services or infrastructures and whenever attacks/incidents involve more than one NREN. Some obvious subjects to address are:

1. Log management: To allow the analysis of available security events the information must be harvested from the systems involved. Transferring all data to centralised SOC tools is one option but it will also cause the transfer of much data that is not really needed. By aggregating and correlating security events based on use cases provided to decentralised concentrators, privacy as well as economic requirements can be met.

2. Log analysis: Almost all NRENs have started to implement some sort of log-analysis system, whether it be open source like ELK, Splunk or some other commercial systems that the local NREN has found useful. As the technology might be different, the attacks and incidents that are applicable will need to be configured to become detectable. This will not only require suitable tools for an automated initial log analysis, but also a shared platform to facilitate the collaborative development and maintenance of the knowledge base needed for any security analyst working in this context.

3. Threat intelligence sharing: While the analysis of security events and incidents will ultimately lead to new knowledge, NRENs and their constituents need new ways of automatically sharing the subsequently developed attack pattern and indicators of compromise (IoCs) as soon as they become available. In addition, the security teams need tools to check past log data for occurrences of such IoCs as well as tools to detect such attacks in the future and to correlate any instance of such attacks without the need for further manual analysis.

4. Big data analytics and machine learning: To support the detection of new attack patterns in security incident and event data, the paradigm of big data analytics and machine learning have shown significant promise. Again, as touched on earlier, other regulations must be considered and ways of adopting existing big data approaches in a compliant way must be identified to increase the security of NRENs and constituents further.

5. Open source intelligence (OSINT): Bundle intelligence from Censys, Shadowserver, Shodan and combine it with own intelligence sources like NetFlow, TLS scans, ZMap scans from within the NREN community. In this way, more detailed intelligence will be obtained. It will also provide a blueprint about what kind of services are put online by the R&E constituency. This will help understand the impact of new common vulnerabilities and exposures (CVEs).

6. Stimulate the cooperation between SOC/CERT entities, not only in NRENs but in the general internet community. Sometimes national initiatives have started, but they are hampered by mistrust of the other ISPs and/or a closed view on how to handle security attacks. Improved, opened-up communication will be stimulated.

7. Provide SOC services for NRENs and/or their constituents.

## 3.4 Vulnerability Assessment 'As a Service'

Some NRENs have incorporated low-impact vulnerability scanning services into their security portals (e.g. DFN utilises OpenVAS to check for critical vulnerabilities on demand and routinely, based on the decision of constituents). But most constituents are deploying local instances of similar scans locally.

By combining GÉANT-wide authentication services, it will be possible to establish a central penetration-testing (pentest) server with a commercial unlimited licence (Nessus, Retina, etc.), which would grant the ability for any CISO for any NREN to perform a pentest on any IP system within their NREN infrastructure. Vulnerability assessment becomes of growing importance, not only to identify vulnerabilities in online information systems, but also to identify all kinds of Internet of Things (IoT) devices connected to the network and campuses that might be vulnerable or in a vulnerable position.

## 3.5 eduVPN

eduVPN enables employees, researchers and students to easily and securely connect to the internet and gain access to their institution's protected systems [eduVPN]. Some NRENs have started eduVPN as early adopters and there is much interest in developing this as a global service. Joint development will allow better and more user-friendly tools to be produced, enabling exchange of trust policies and trust anchors for cross-NREN access.

## 3.6 Other Solutions and Services

Other potential solutions and services that were mentioned during the consultations are:

- Sharing of consolidated security information and threat intelligence feeds.
- Vendor score database.

- AI for security data.
- Nessus reporting template.
- Vulnerability management tool.
- Enabling exchange of trust policies and trust anchors for cross-NREN access.
- Working group on information sharing and security standards for procuring (networking) equipment.
- Standards for procuring (networking) equipment.
- IoC detection and sharing at institutional level.
- Information sharing platform (real-time information / threat sharing).
- Best practices for using TCS for client security (email).
- Agreements for inter-country collaboration: trusted frameworks/standards.
- Assessment of correlated security events and reputation score for e.g. IP addresses (RepShield), further development and distribution in multi-domain manner.
- Development of new types of sensors and integration in aggregation platform (e.g. honeynet, host/network IDS and content filter, etc.).
- Quantum cryptography and Blockchain.
- Coordinating the implementation of security controls such as RPKI and BGPsec to protect against route hijacking and operational mistakes affecting routing resulting in widespread outages.

## 3.7 Planned Benefits and Impacts to the User Community

All NRENs have limited resources to develop security solutions and services. Most have picked special areas of interest depending on the needs of the own organisation or of their constituents, or depending on available prototypes (e.g. from other research projects like eCSIRT.net or ACDC), individual preferences (e.g. network vs. host expertise), knowledge and experience. Not all the services will be the 'new eduroam' and be useful for all users within all NRENs, but most of the services will be beneficial for the NRENs and their constituents. By combining efforts and focusing on NREN-compatible solutions, the 'time to market' as well as the available functionality can be vastly improved. Experience has shown that while commercial tools are working for many commercial entities, the market for very large-scale infrastructures, with millions of users and higher numbers of IP addresses by a factor of 5 to 10, is rather limited and the value of commercial off-the-shelf products (such as expensive DDoS detection and mitigations products) is low compared to the costs, both procurement and operational. Services developed by NRENs for NRENs, which provide the needed scalability and make economic use of the available budget, are the key for securing the NRENs' security and supporting their security teams.

The NRENs will benefit firstly from shared experiences and knowledge of what has already been done by the other NRENs and, secondly, from the innovation and development of new solutions and services that would otherwise not be available. Integration of commercial products that have been thoroughly tested and proved in operational settings will augment this self-supporting approach.

## 3.8 Implementation

There is a large demand for security solutions and services. To start with, existing solutions and deployed products need to be assessed and evaluated, taking into account the needs of a large user base or the scale of cross-border NREN collaboration and support. Thereafter, the priorities,

requirements and principle commitment for new solutions, extensions, improvements and integration need to be identified and assessed. Based on such assessments, the actual development can be supported and organised. To foster the information exchange and allow a continuous assessment of new ideas or needs, working groups will bring together developers and operations teams, including not only CERTs or SOCs but also NOCs and internal service providers.

# 4 Legal and Privacy Compliance

**Main goal**: to work together in monitoring and implementing the EU and other regulations on security, privacy and data sharing, and in representing NRENs in influencing what the regulations will be about in the future.

Legal compliance gets more important as regulations are becoming more widespread. The reason for that is the importance of cybersecurity for a widely digitised society and economy, and industries, such as the emerging IoT industry, not placing much emphasis on basic security for their (connected) products. The basis of digitalisation is trust. Local and global legal and privacy compliance needs to be managed as a part of the above-mentioned frameworks and compliance risks are part of the risk landscape.

There is a growing volume of legislation that tries to regulate ICT, (open) data, intellectual property, privacy, identity and open access. Though much of the preparation for the General Data Protection Regulation (GDPR) [GDPR] has to be done before May 2018, the process will not be completed for some years to come. First, there are many legacy and proprietary systems that it will take more time to make compliant. Second, the GDPR implementation is not a one-off activity; enforcing privacy regulations on all GÉANT community systems and the systems of partners and suppliers is a continuous effort.

New EU regulations, such as eIDAS, and derived or separate local regulations, such as the Dutch Generic Digital Infrastructure regulation, will have a large impact on, for example, identity management and identity federations, for both the NRENs and their constituents.

Regulations or procedures that are of mutual concern include (but are not limited to):

- GDPR, data registers, security compliance checklists, 'information policies'.
- ePrivacy Directive [ePrivacy].
- NIS Directive [NIS].
- Guidelines for international cooperation (for example, for big data transfers).
- Export restrictions (threat detection and information exchange).
- Horizon scanning for future legislation.

## 4.1 Planned Benefits and Impacts to the User Community

The EU regulations apply to most of the NRENs, therefore it makes sense to join forces in influencing the design and development of new regulations, analysing the impact and identifying efficient ways of implementation. As with most subjects, there will be NRENs that adopt new regulations in the early stages and others that join slightly later. This activity will ensure an effective knowledge exchange and sharing of best practices.

GÉANT and the NRENs will benefit from keeping a register of current and upcoming legislation and its impact, especially if analysis of scope and impact is followed by a non-legal explanation of what a piece of legislation means for the GÉANT community's business and services.

New legislation does not require changing the way the community does business overnight, but it needs to be carefully analysed in the context of GÉANT and the NRENs. Best practices for implementing new or changed legislation need to be developed and shared by jointly using the scarce legal resources.

The main focus will be on GÉANT and the NRENs. However, the platforms and communities that are involved with legal compliance will also be invited to share and develop materials for constituents.

*Limitation: within this subject, the efforts will be limited to legislation that has direct impact on the core operations of GÉANT and the NRENs, excluding any financial or administrative legislation.*

## 4.2 Implementation

The proposed approach to implementing legal and privacy compliance includes:

- Continue the Task Force on Data Protection Regulation (TF-DPR) as a Special Interest Group (SIG).
- Monitoring of developments and new legislation by expert group of legal officers.
- Collect, analyse and regroup good practices into best practices and publish.

The topics suggested by the community include:

- GDPR security issues checklist (rated as the most urgently needed by the community during consultations).
- Data register (art.30 GDPR).
- Non-legal compliance framework (Sirtfi, ISO, etc.).
- NIS Directive.
- Guidelines for big data transfers.
- Future legislation – horizon scanning.
- Export restrictions (malware exchange) (very low score from the community).
- ePrivacy Directive (very low score from the community).
- Multiple contracts for the same service (very low score from the community).
- Security compliance of services provided by GÉANT and NRENs (such as eduroam, (cloud/IaaS) framework products, community clouds, PaaS/SaaS conformance, etc.).

# 5 Management of Risks

**Main goal**: prepare a set of commonly used processes, templates, guidelines and procedures that can be used by GÉANT and the European NRENs to better manage risks.

Risk management is crucial in order to define the future objectives of an organisation and community as a whole and to enable sustainability. While NRENs need to manage many risks, including organisational risks related to financing, etc., the target of any activities described within this white

paper is risks associated with the safety, privacy and security of users, organisations and infrastructures.

Effective NREN-specific risk management strategies and tools would help the NRENs to achieve their goals by proactively identifying and analysing risks, threats and vulnerabilities, and responding to risk in an iterative process, looking at all aspects of security – confidentiality, integrity and availability – for the organisation and its products and services, and for the technical infrastructure.

There are existing risk management standards and some of the NRENs are adopting them (or parts of them) in their practices, but a dedicated effort is needed in order to prepare and implement a common baseline for NREN risk management processes and to ensure adoption of this throughout the NRENs and GÉANT.

Collaborating and sharing best practices have been identified as the most important ways of achieving the desired results. Setting up a joint risk and threat catalogue and sharing actual (operational) threat information have also been identified as a high priority for which processes need to be developed and tools selected and combined.

## 5.1 Planned Benefits and Impacts to the User Community

As there are many risks associated with security, safety and privacy, and as such risks continue to increase, NRENs are starting to find it necessary to implement some sort of formal institutionalised risk management system.

Only a few NREN organisations already have an established, complete and effective risk management framework in place; most are still struggling with choosing a manageable risk management approach and integrating it into their organisations. Not all NRENs have the people, tools, policies and procedures needed to mitigate risks, and even those that do could benefit from consensus on some common NREN-specific system and a shared, common catalogue of risks, assessment of identified threats and risks, and overview of threats facing NRENs and their constituents in general, as well as agreed mitigations.

This activity would be beneficial for the NREN community on multiple levels. One of the intended benefits is the creation of risk management and reporting standards, including common structure, policies, processes and terminology when talking about risks internally and externally. There are countless risk assessment and management templates and guidelines available and some of the NRENs (still far from many) have successfully adapted them for their specific needs. These could be used as examples and the lessons learned could form the foundation for the other organisations' individual or group guidelines and templates for risk management, assessment and authorised non-compliance. The work that NRENs do is largely similar and so are the challenges and problems that they face. Therefore, they would benefit from collaborating and sharing information on registration and management of risks in risk management modules and information security controls. Furthermore, it would be beneficial for the NRENs to develop a common risk catalogue, to which they could refer when planning their risk management processes.

Another benefit for the NREN community, including its constituents, would be the creation of a more risk-focused culture in European NRENs that would shape the decisions of management and employees. The more common risk discussions become, the less the chance that high-profile problems might occur and possibly even affect other NRENs or a wider GÉANT community. Joint risk awareness

and risk analysis workshops and risk assessment sessions with NREN staff, management and board members would contribute to creating widespread risk awareness within and between NRENs.

The user community would also benefit greatly from increased joint threat- and intelligence-sharing efforts. Having access to timely information about emerging risks and new threats is extremely important in cybersecurity as it can help in detecting and preventing upcoming attacks and security incidents caused by such attacks.

Sharing information, knowledge and experiences needs to work on two levels:

1. Knowledge and insights regarding threats and vulnerabilities that might be exploited and cause major changes in the associated risks and which need to be registered in the risk catalogue and be assessed.

2. On the operational level, the sharing of attack patterns, incident-related data and indicators of compromise needs to be automated and institutionalised as part of incident management activities and/or business continuity planning (see below).

Both levels could be based on two scenarios of automated sharing: peer-to-peer and with a central coordinator.[2]

In addition, working on and promoting a wider use of tools such as MISP, Warden or other threat-sharing instruments would be another important step towards the (automated) mitigation of identified risks and threats, beneficial to the user community.

Not many NRENs currently have a risk management strategy in place that would be suitable for the specific needs of the community; implementing one, with the necessary people, tools, policies and procedures identified and agreed upon, would have a positive impact on individual organisations and the GÉANT community as a whole.

## 5.2 Implementation

Risk management activities should be carried out throughout the period of 2019 – 2022, beginning with sharing best practices and collecting existing tools, templates and guidelines, building on the work that is currently being done by the SIG-ISM Risk Management working group.

Topics that should be included in the implementation plan (suggested by the community during the consultations) are as follows:

- Risk assessment template/guidelines.
- Risk and threat catalogue.
- Risk management template/guidelines.
- Risk assessment and authorised non-compliance templates.
- MISP and other threat-sharing instruments.
- Risk assessment sessions with NRENs (board, management).
- Risk of outsourcing – measured by contracts, laws (very low scores from community).
- Risk management outside Europe (very low scores from community).

[2] This topic, as well as analysis and collaborative defence, is the aim of the PROTECTIVE project [Protective].

# 6 Training and Awareness

**Main goal**: continue developing security-related trainings and training packages to meet NREN needs and compiling an extensive list of trainings and materials for the NREN community available elsewhere, on affordable terms. In addition, collect, and also develop, suitable security awareness materials and best practices, as there is a severe lack of existing materials, in order to create a security culture across the community. Though the main target audience is the NRENs, many of the materials may also be suited to and used by the constituents.

The need for security-related training for the NREN community is evident. The best example would be TRANSITS trainings – the waiting lists start building up a few months prior to the actual sessions. Similarly, the training sessions offered at the TF-CSIRT meetings, such as the OSINT training, fill up quickly. The NREN security community has a lot of expertise and knowledge that could be collected and organised into one-off trainings or training series, by using the most up-to-date training methods and technologies. More materials need to be developed in order to offer the most relevant security and incident response training for different NREN staff groups, from security professionals, to security officers and management.

In order to achieve that, it is important to continue working together with the community experts, other security organisations such as FIRST and the private sector; to share best practices between NRENs and other organisations; and continuously look into new ways and opportunities for training, such as online courses or simulations enabling new ways of interaction and experiences.

## 6.1 Planned Benefits and Impacts to the User Community

Improved security and security awareness are without a doubt the main benefits of security training. It is relevant for all NRENs in Europe and beyond, and has a great impact on the NREN security culture.

Many training resources and events, especially commercial, are already available. However, some of those might be in a language other than English, or for some NRENs they might not be affordable. One of the aims of this activity would be to make and continuously update an incident response and security awareness training inventory, listing the most relevant training, combining training and awareness materials developed by NRENs and other institutions, translating those if needed, grouping them in categories. This would make it easier for the user community to find relevant affordable training and share the materials that they develop themselves with their peers. It is important to keep in mind that security is a fast-changing topic, so a significant effort has to be put into continuously reviewing and updating the materials.

In addition to collecting information on the training events and resources, this activity would also focus on assessment of training needs and creation of new training and materials. It is evident that different levels of training are required by the community: security staff (expert) training, training and creating awareness of other staff members, and security-related training for management and board members. The most up-to-date trainings for security experts on the latest trends and threats are necessary to increase the capacity to adopt the new technologies and methods, and also to train them in other skills, such as communication and training others. This activity would add to the expert training that is already available, such as TRANSITS II and Train the Trainer, after consulting the community on what further skills and knowledge are required.

In order to establish a common security culture, all other staff members should also receive training that would create and increase awareness. The NRENs would benefit from having confident staff and a culture where security is everyone's responsibility. By using the best examples from the community and beyond, the aim is to create interesting and relevant training for the NREN staff members that would outline what each one of us must do in order to secure the environment and information that we are working with.

Training for management and board members is also a priority. This should be a separate category because the knowledge and skills required are different from those of the security experts and the rest of the staff. The most relevant topics for this group are legal and organisational, and to start with, the materials could be based on the equivalent modules of TRANSITS I training.

Use of the newest technology and training methods in order to make the training more affordable and accessible is extremely important. For this it is essential to work together with the learning and development professionals during all stages of the activity in order to make and present the materials in the most advanced and innovative manner, starting with considering what can be adopted as online courses or applications.

The main benefit for the community will be a common security culture across all levels of organisations, confident and aware staff, and the best security professionals, ready to face the current challenges and support the rest of their organisation.

## 6.2 Implementation

This activity will consist of training needs assessment, delivering series of courses, development of commonly used materials, conducting security awareness campaigns, and the creation and maintenance of an incident response and security awareness training inventory.

Topics may include:

- Shared training materials (e-learning, posters, films, etc.).
- Crisis management training/workshop (also mentioned in Section 7).
- Risk management training/workshop (also mentioned in Section 5).
- Protecting personal data workshop.
- Management/board training (TRANSITS-like training for management level).
- Setting up awareness tools catalogue.
- Phishing awareness.
- Secure Code Training and Secure Code Audit for general services and their developers.

# 7 Incident Response, Business Continuity and Crisis Management

**Main goal**: make sure that GÉANT and the NRENs can adequately and in a timely manner respond to complex incidents, control the resilience of the main processes and infrastructure, and are able to handle a complex crisis in an organised fashion.

No matter how well organisations prepare, incidents will always happen, and incidents will sometimes evolve into crises. Therefore, steps must be taken to ensure that GÉANT and its member organisations are prepared for them: that all relevant processes are in place, staff are well trained and crisis procedures are rehearsed on a regular basis. And last but not least, organisations must make sure their infrastructure is robust, with built-in resilience.

This subject area addresses the incident response, business continuity and crisis management processes and procedures, the design and implementation of these processes, and the essential training and exercises. Security incident response is traditionally well organised for NRENs, with trainings, an active TF-CSIRT community, the Trusted Introducer service and the corresponding certification scheme. However, for most NRENs this incident response process is only aimed at the network and at network services for the constituents, not at the internal processes of the NREN or at other ICT services an NREN offers.

Similar efforts in the WISE collaboration community for e-infrastructures support efficient security incident handling; equally, REFEDS is promoting adequate incident response. Adoption, however, is still of some concern, as is crisis management and incident and crisis coordination within an organisation, NREN or constituent, and across organisations, both nationally and internationally. Since the interests of GÉANT and the NRENS cross borders on a global scale, global coordination and guidelines are much needed.

Security incidents and crises evolving from them will become of increased complexity, spanning both network and value-added services, their management equally so, not least due to new legislation such as mandatory data breach notifications.

In the GÉANT CLAW crisis management workshop in November 2017 in Malaga, 40 participants expressed active interest in developing common practices, processes, procedures and exercises for crisis management in NRENs. There is a growing demand for joint crisis exercises and trainings.

## 7.1 Planned Benefits and Impacts to the User Community

The main benefits of this activity are that GÉANT and the NRENs will improve their capabilities to efficiently respond to security incidents of all kinds for all their services, and that they will be able to respond to a crisis in a manner that minimises the impact of the crisis, no matter what its nature, for the user community, and that resolves the crisis quickly and in an organised matter. The user community will also benefit from this activity as the reliability of services (of all kinds) will be of the highest possible standards, despite security incidents or small or larger crises, and services will be restored quickly after a major local or international crisis.

Inefficient processes and single points of failure will become apparent during exercises and analysis, allowing GÉANT and individual NRENs to identify and implement improvements. To help with improvements, best practices for processes and resilience will be made available, standardised but not prescribed, allowing room for local adoption.

In addition, conducting local and joint crisis exercises will enable crises to be addressed more efficiently and the cooperation between NRENs and between GÉANT and the NRENs to be tested. Best practice for setting up and maintaining a crisis management organisation will be developed and made available, practical exercise scenarios for NRENs to conduct themselves will be provided, and a bi-annual multinational NREN cyber-crisis exercise will be introduced.

These exercises will ensure that awareness of crisis management is a priority throughout the community, that all NRENs have the tools and guidelines to form or enhance their crisis management plans and procedures, and that a common understanding and terminology to deal with crises on a European (and, long term, a global) scale are created.

The exercises will be used:

- To test whether participating organisations are prepared.
- To evaluate the best practices for incident response, crisis management and business continuity.

## 7.2 Implementation

This subject will run throughout the whole GN4-3 period, as shown in Table 7.1 below.

| Area of Activity | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| Best practices for crisis management and incident response | Collect good practices and compile into best practices | Implement best practices at 3 NRENs, workshop | Implement best practices at 3 NRENs, workshop | Implement best practices at 3 NRENs, workshop |
| Crisis exercises – NRENs | Develop 2–4 small exercise scenarios on both incident response and crisis management + workshop | Develop 2 small exercise scenarios + workshop | Develop 2 small exercise scenarios + workshop | Develop 2 small exercise scenarios + workshop |
| Crisis exercises – European | Annual European crisis exercise | Annual European crisis exercise | Annual European crisis exercise | Annual European crisis exercise |

Table 7.1: Summary of proposed incident response and crisis management activities during GN4-3

Topics may include (suggested by the community during the consultations):

- Model process and policy descriptions.
- Best practices for incident response processes, business continuity planning and crisis management.
- Workshops on interdependency and business continuity controls.
- Crisis exercises and crisis simulation.
- Integrating security incident response with handling of data breaches and other privacy-related processes.

# 8 Annexes

The following action templates are associated with this white paper:

- Annex 1: Baselining for Products and Services and Organisations [ANNEX1]
- Annex 2: Firewall on Demand [ANNEX2]
- Annex 3: Centralised DDoS Mitigation [ANNEX3]
- Annex 4: SOC Operations and Tools [ANNEX4]
- Annex 5: Vulnerability Assessment (as-a-service) [ANNEX5]
- Annex 6: eduVPN [ANNEX6]
- Annex 7: Other Security Products and Services [ANNEX7]
- Annex 8: Legal and Privacy Compliance [ANNEX8]
- Annex 9: Management of Risk [ANNEX9]
- Annex 10: Training [ANNEX10]
- Annex 11: Awareness [ANNEX11]
- Annex 12: Incident Response, Business Continuity and Crisis Management [ANNEX12]

# Acknowledgements

The authors would like to thank the contributors to and reviewers of this white paper and those who helped with the process:

- Hank Nussbacher (IUCC)
- Klaus-Peter Kossakowski (DFN)
- Ralf Groeper (DFN)
- Christine Kahl (DFN)
- Remco Poortinga - van Wijnen (SURFnet)
- Paul Howell (Internet2)
- Tomáš Čejka (CESNET)
- Ossi Kuosmanen (CSC)
- Robert Hackett (HEAnet)
- Claudio Allocchio (GARR)
- Rogier Spoor (SURFnet)
- Eduardo Jacob (EHU – University of the Basque Country)
- Albert Hankel (SURFnet)
- Stefan Metzger (Leibniz Supercomputing Centre)
- Tom Crumpton (REANNZ)
- Martin Leuthold (SWITCH)
- Tangui Coulouarn (DeiC)
- Nicole Harris (GÉANT)
- Brook Schofield (GÉANT)
- Casper Dreef (GÉANT)
- Evangelos Spatharas (GÉANT)

# References


[ANNEX1] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex1-Security%20Baselining.pdf

[ANNEX2] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex2-Security-Firewall%20on%20Demand%20(FoD).pdf

[ANNEX3] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex3-Security-Centralised%20DDoS%20Mitigation.pdf

[ANNEX4] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex4-Security-SOC%20operations%20and%20tools.pdf

[ANNEX5] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex5-Security-Vulnerability%20Assessment.pdf

[ANNEX6] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex6-Security-EduVPN.pdf

[ANNEX7] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex7-Security-other%20security%20products%20and%20services.pdf

[ANNEX8] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex8-Security-Legal%20and%20Privacy.pdf

[ANNEX9] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex9-Security-Management%20of%20Risk.pdf

[ANNEX10] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex10-Security-%20Training.pdf

[ANNEX11] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-%201-3-2018/Security%20White%20Paper/Annex11-Security-%20Awareness.pdf

[ANNEX12] https://intranet.geant.org/gn4/2/Activities/NA1/GN4%20Documents/PMO%20Documents/2018%20White%20Papers/White%20Papers%20-

%201-3-2018/Security%20White%20Paper/Annex12-Security-%20Incident%20Response.pdf

[EC-JOIN-450] *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Brussels, 13/09/2017, JOIN(2017) 450 final http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&from=EN

[eduVPN] https://eduvpn.org/

[ePrivacy] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32002L0058

[GDPR] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[GÉANT-Strat2020] *GÉANT Strategy 2020: Over the Horizon* https://www.geant.org/Resources/Documents/Strategy2020_Over-the-Horizon.pdf

[GN4-3_SecPlanning] https://wiki.geant.org/display/GSP/GN4-3+Security+Planning+Home

[NIS] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[Protective] https://protective-h2020.eu/

[Reviewers] https://wiki.geant.org/display/GSP/List+of+reviewers

[SecGroups] https://wise-community.org/2017/07/31/security-is-the-new-black-of-the-re-community/

# Glossary

| | |
|---|---|
| **ACDC** | Advanced Cyber Defence Centre |
| **AI** | Artificial Intelligence |
| **BGPsec** | Border Gateway Protocol – Security extension |
| **CERT** | Computer Emergency Response Team |
| **CISO** | Chief Information Security Officer |
| **CLAW** | Crisis management exercise for the GÉANT community |
| **CSIRT** | Computer Security Incident Response Team |
| **CSO** | Community Support Office |
| **CVE** | Common Vulnerability and Exposure |
| **DDoS** | Distributed Denial of Service |
| **DoS** | Denial of Service |
| **EC** | European Commission |

| | |
|---|---|
| **eCSIRT.net** | European CSIRT Network |
| **eIDAS** | electronic Identification, Authentication and Trust Services |
| **ELK** | Elasticsearch, Logstash, Kibana |
| **ENISA** | European Union Agency for Network and Information Security |
| **ETSI** | European Telecommunication Standards Institute |
| **EU** | European Union |
| **FIRST** | Forum of Incident Response and Security Teams |
| **FoD** | Firewall on Demand |
| **GDPR** | General Data Protection Regulation |
| **HE** | Higher Education |
| **IaaS** | Infrastructure as a Service |
| **IDS** | Intrusion Detection System |
| **ICT** | Information and Communications Technology |
| **IoC** | Indicator of Compromise |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **ISO** | International Organisation for Standardisation |
| **ISP** | Internet Service Provider |
| **IWGDPT** | International Working Group on Data Protection in Telecommunications |
| **KPI** | Key Performance Indicator |
| **MISP** | Malware Information Sharing Platform |
| **NA** | Networking Activity |
| **NA3 T5** | NA3 Partner, User and Stakeholder Relations, T5 Task Forces and Special Interest Groups |
| **NIS** | Network and Information Systems |
| **NIST** | National Institute of Standards and Technology |
| **NOC** | Network Operations Centre |
| **NREN** | National Research and Education Network |
| **OSINT** | Open Source Intelligence |
| **PaaS** | Platform as a Service |
| **R&E** | Research and Education |
| **REFEDS** | Research and Education Federations |
| **RPKI** | Resource Public Key Infrastructure |
| **SaaS** | Software as a Service |
| **SCI** | Security for Collaborating Infrastructures |
| **SIG** | Special Interest Group |
| **SIG-ISM** | SIG on Information Security Management |
| **SIM3** | Security Incident Management Maturity Model |
| **Sirtfi** | Security Incident Response Trust Framework for Federated Identity |
| **SOC** | Security Operations Centre |
| **T** | Task |
| **TCS** | Trusted Certificate Service |
| **TF** | Task Force |
| **TF-CSIRT** | Task Force on Computer Security Incident Response Teams |
| **TF-DPR** | Task Force on Data Protection Regulation |
| **TLS** | Transport Layer Security |
| **TRANSITS** | Computer Security and Incident Response training |