Contribution ID: **28** Type: **not specified**

# Information Security 3: Who you gonna call?

*Monday, 6 May 2019 16:00 (15 minutes)*

Have you ever wondered why the security team makes so much fuss? Why can't I just get on with my work? Why do I have to urgently patch my services? I am involved in Open Science, I don't need security!

The EGI CSIRT hears such statements all the time. During these five short talks (one per conference track) at the EGI Conference 2019 we will explain all! Our aim is to make the need for "security"clearer and to explain why the EGI CSIRT does what it does.

In each of the 5 talks, we will share an amusing but instructive "War story"or two, relevant to the particular track, demonstrating the problems that can occur when security breaks down. Services may cease to be available or data may be lost or corrupted. We will follow this with details of our security controls aimed at protecting against such an event happening again.

Cybersecurity attacks are an ever-growing problem and we must act to both reduce the security risk and to handle security incidents when they inevitably happen.

There is no one way of preventing security incidents, but a range of security controls can help reduce their likelihood. Commercial cloud infrastructures sell compute and storage. Whether the cycles are used by the paying customer, or if the service the user runs on the infrastructure is available is of secondary interest, and the responsibility is shifted to the customer. In e-Infrastructures like EGI, we have more control over who can access the infrastructure and their allowed actions. The emphasis is to support users in making sure the infrastructure they use or the services they run are indeed used for the intended purpose.

The first line of defence is policy, which states what the various parties which interact with the infrastructure can and cannot do.

The choice of technology used on the infrastructure is also important, to ensure it does not have obvious security problems, can be configured to comply with security policies and is under security maintenance. It is important that any software vulnerabilities discovered are fixed by the software provider in a timely manner, and that patches are deployed appropriately.

Data centres that host the distributed infrastructure should be managed and configured securely. We deploy monitoring to ensure that they, for example, are not running software known to have serious security problems. Another EGI CSIRT activity is to assess incident response capabilities, via security exercises, known as Security Service Challenges. EGI services should provide sufficient traceability of user actions as well as interfaces to their systems that offer methods needed to contain an incident, e.g. the suspension of credentials found in activities violating security policies.

Fundamental to our approach is the performance of regular security risk assessments, where threats are identified and the likelihood and impact of these occurring are assessed. The results are used to identify places where additional effort is required to mitigate the important risks.

## Type of abstract

Presentation

**Primary authors:** KOURIL, Daniel (CESNET); Dr CROOKS, David (STFC); GROEP, David (NIKHEF); KELSEY, David (STFC); CORNWALL, Linda (STFC); Dr GABRIEL, Sven (NIKHEF); BRILLAULT, Vincent (CERN)

**Presenter:** GROEP, David (NIKHEF)

**Session Classification:** Implementations of AAI