Security training and awareness subjects

Subject	Target group
Laws & Regulations (privacy, data protection, export)	Management, governance, admin, users
Secure Software development	User, user coordinator, contractor
System hardening	System admin, network engineering
System operations	System admin, network engineering
Monitoring and logging	System admin, network engineering, response teams
Forensics	Response teams
Incident respons and analysis	Response teams
Contigency planning and disaster recovery	Management, governance, admin, user coordinator, response team
Organisation, roles, responsibilities (generic introduction)	All
AAI proces and procedures, FIM, SSO	System admin, user coordinator
Systems design	Architect, network engineer
IT security awareness for users	Users, user coordinator, all
Developing and maintaining policies and procedures	Management, governance
Applying policies and procedures	Architect, system admin, user coodinator
System acquisition	Acquistion
Decommissioning (data leakage prevention)	Admins, governance, user coordinator
Risk management	management, governance, respons team, admin

Laws & Regulations (privacy, data protection, export)

When setting up and operating an E-infrastructure you should know what laws and regulations you have to comply with. These will be different depending on the kind of data that is processed and possible depending on the international partners. Management and governance need to have an overview of what rules and regulations apply, admins need to know what these laws and regulations mean for systems configuration and operations. Example regulation subjects are, (not limited to) dataprotection, non-proliferation, technology export, law enforcement.

Users must be informed on applicable laws and regulation and on what they mean for them.

Secure Software development

Training withing this group should focus on all the aspects related to software programming from the security point of view. It should include integrating security practices into the software development lifecycle and verifying the security of internally developed applications before they are deployed. This will help to mitigate risk from internal and external sources. Security practices which should be included are: design, construction, testing, release, and response.

One of the important steps in secure development is integrating testing tools and services into the software development lifecycle. The training could describe or train on tools allowing developers to model an application, scan the code, check the quality and ensure that it meets regulations. Furthermore, automated secure development testing tools that find and fix security issues could be elaborated.

Additionally secure development trainings could be offered certifying experience in secure development.

See e.g.: http://www.sans.org/curricula/secure-software-development

System hardening

Any system providing ressources to the outside world is on risk to be hacked. Often simple security tools are installed and used by default like local firewalls, virus scanner etc., but even with these security measures in place, computers are often still vulnerable to outside access. System hardening, also called Operating System hardening, helps minimize these security vulnerabilities.

The trainings offered should provide detailed trainning on those tasks eliminating as many security risks as possible. The trainings should include e.g. technics to check for non-essential software programs which can be removed from the system, since they could provide "back-door" access to the system. Guest accounts should be closed, alternate boot devices disabled, only secure passwords allowed, no remote root access, monitoring of unauthorized access attempts, etc.

System operations

Training should focus on providing secure services to the user community. This includes but is not limited to secure authentication and authorization practices, recognizing breaches, scanning for vulnerabilities, change management, patching, logging, intrusion detection, incident response, disaster recovery, and forensic practices.

Service lifecycle and secure practices during of each stage should be covered in-depth. These stages include requirement gathering, technology investigation, development, testing, deployment, production operation and retirement. It should also cover transitioning between stages.

Monitoring and logging

Monitoring and logging are the essential components which allow to track system events in their historical order. Without monitoring you are not able to be aware of any events going on in your system. Having found suspicious system behaviour must ultimately lead to further investigations, which normally are able only if extended logging has been done continuously.

The training will/should provide an overview about available monitoring and logging tools, central system logging and techniques used to analyse those combined loggings. Only centralized logging helps to combine system and network activities and get a comprehensive look on the overall attack.

Forensics

Forensic analysts collect, preserve, and analyze digital evidence during the course of an investigation. Forensics includes but is not limited to system and user behaviour, file system content, communication patterns etc. There are a lot of techniques and tools out there, which can help to investigate on an suspicious activity within the system. The trainings should help system and network admins to doing their day to day business with the safeness on board to being wapponed against threads coming from the outside world.

Incident response and analysis

Any outward facing service provides a potential attack surface. Incidents should be expected by users, administrators and response teams. Proper response and analysis is critical to reduce continued risk. All levels of an E-Infrastructure should know exactly how to handle an incident. This starts with what to do with the service in question to preserve important forensic information, who to contact in event of a breach or attack, how to limit unfavorable consequences, and how to notify the community of the incident. This will also include contacting collaborating E-Infrastructures to be sure they are not also affected by the breach or attack.

Training should focus on properly handling security events. As many projects are now multi-institutional and multinational building trust and notification channels with collaborating E-Infrastructures should also be covered. Incident processes (if/when to make public, when to close) and announcement procedures (who to contact, how to contact, etc.) frameworks should be discussed.

Contingency planning and disaster recovery

As infrastructures grow more complex incidents and incident causes can grow more complex and will have more impact. E-infrastructures should prepare for recovery after major incidents that cause the temporary or permanent loss of critical parts of the infrastructure. As a part of the preparation there should be a crisismanagement organization and (at least) high level recovery plans. To be able to do a successful recovery documentation and data should be available through proper backup mechanisms. All recovery facilities including backups should be tested at regular intervals.

E-infrastructures should also look into prevention against complex incidents and take basic measures such as power backup, fire prevention and suppression systems, lightning protection and where applicable protection against natural disasters like earthquakes and floodings.

Organisation, roles, responsibilities (generic introduction)

High level introduction to security concepts tailored to organizational goals. This would touch on many of the aspects of other subjects by defining them, offering examples, and increasing awareness of organizational policy related to information security. This training should not attempt to cover technical details which are covered in other subjects, but should give the user a sense of the importance of information security and cover any policy necessary for the user to meet organizational requirements. It should also prepare the trainee to deal with any security emergencies they may encounter and give them the background to make sound information security choices.

AAI processes and procedures, FIM, SSO

Setting up an overall authentication and authorization infrastructure is a comprehensive task already. A lot of processes have to be defined, setup and managed. Those processes become much more complicated when dealing with collaborative environments. Here several partnes with their own authentication systems policies and procedures have to agree on common principles and procedures. Federated Identity Management (FIM) will come into the game and since the user doesn't want to authenticate several times at different systems a global single-sign-on (SSO) solution would be preferable.

Trainings of different kinds could be offered starting from AAI in local organizations up to management platforms for collaborative environments. The traing should investigate on those areas and provide the participant with hands-on information. how to set-up those AAI infrastructures.

Systems design

This training should provide insight to secure system design concepts. These could include some set if not all of the following concepts as well as including others important to the organization or stakeholders.

- Least Privilege - A subject/program should be given only the minimum set of privileges necessary to complete its task
- Fail-Safe Defaults - Unless a subject is given explicit access to an object, it should be denied access to that object
- Economy of Mechanism - Security mechanisms should be as simple as possible
- Complete Mediation - All accesses to objects must be checked to ensure that they are allowed
- Open Design - The security of a mechanism should not depend on the secrecy of its design or implementation
- Separation of Privilege - A system should not grant permission based on a single condition
- Least Common Mechanism - Mechanisms used to access resources should not be shared
- Psychological Acceptability - Security mechanisms should not make the resource more difficult to access than if the security mechanism were not present
- Multiple Lines of Defense – Increase odds that no single vulnerability is common to all functionality

Reference: http://web.mit.edu/Saltzer/www/publications/protection/index.html

IT security awareness for users

Many of the research results produced will be publicly available. But also sensitive and confidential information pertaining to research, partners and employees are worked on. If these informations would become public, there would be significant damage. So protecting this sensitive information is of highest priority.

IT security has to identify the threats to such sensitive IT resources and determining appropriate technical and organizational measures to protect them.

Since attackers have begun to focus on the weakest link in the security chain: the person sitting at the keyboard have to be trained accordingly.

Over 70% of successful attacks require the active cooperation of the user. Technical measures for IT security only work properly when employees and management use them appropriately and do not wittingly or unwittingly circumvent them.

The training should describe the most important rules, tips and tricks for securely using IT systems by non- IT-security-affin personal and especially make them aware of the risks coming up when using the world wide network.

Training areas could include:

- Hot Topic Phishing and Tips for using e-mail
- Secure passwords and Tips for using passwords
- Viruses and Trojans and Protection against them
- Advice for securely using cloud services and social networks
- IT security at home and while travelling

Developing and maintaining policies and procedures

The risk an organisation will commit itself to is highly dependend on the security policy it wants to implement. If no access from outside is offered, only internal weak point have tob e considered.

The other way round, a very open organisation provides numerous attack points to external intruders.

The training should provide an overview about different kinds of IT security policies, the risks associated with those, and the security tools available to cope with those environments. Furthermore there should be hints how to maintain the installed procedures. Since it is also required to have the defined security level up and running all the time, hints should be given also how IT security awareness of staff members and users can be periodicly refreshed.

Applying policies and procedures

Every organisation has setup its own IT security policies and procedures. All systems installed in this organisation have to apply to those policies. Therefore it is the task of any system administrator to implement these policies in a way that they are compliant to the intended security level.

The traing should provide an overview about default policies and procedures implemented out in the field and give hints how to handle those scenarios in a comprehensive way. After participating to the training the system administrator should be able to map the relevant organisational security policies to the system tools available in the corresponding systems.

System acquisition

The acquisition of a system can be structured into different areas spreading from budgetarian issues (purchasing the system), needed space, cooling, power consumtion etc. Most often the security aspects are neglected Is the system to be purchased the right one for the environment where it should be used and for the tasks to be fullfilled? Where some systems provide very good security features out of the box, others have to be adapted with a lot of effort. Some system designs are optimized for intranet usage only whereas others fit excellently in distributed envoironments.

The trainings offered should give the participants an overview about system architectures fittting into the one or the other scenario making it easier to decide for the best fitting architecture.

Decommissioning (data leakage prevention)

Setting up a system is straight forward, but decommissioning the system might become much more complex. It is not just turning off power. System decommissioning includes freeing the system of any user data by providing processes how to do those transfers and setting up a logical time schedule for doing so. Any priviledges offered have to be withdrawn, disk drive content has to be deleted in a professinal manner etc.

The training should give an overall overview about the tasks to be fullfilled by system admins on the system itself as well as the tasks to put in place for freeing organisational ressources, e.g. deleting user info in AAI infrastructures etc.

Risk management

When controlling security you need to know what risks you need to control. A risk analysis and an associated risk management process will support making the right choice for security measures. A risk analysis is aimed at identifying and quantifying risks, the chance and the impact of risks. There are several methods and standards that can be used to analyse and manage risks. Risk management can be on a broader scope for the whole system but can also be used to analyse the impact of an incident in a structured way.