Good security management

Companies & organizations

INTRODUCTION

A robust security organization relies on a number of factors. However, there are four basic elements that must be defined when laying the foundation for the continued security efforts of your organization: roles and responsibilities, security plans and reporting, security culture and crisis management.

In your efforts to implement these measures, it is important that you remain aware of already existing structures, and duly assess whether the measures should be implemented at the central or local level.

Use the question lists to assess the current state of your security management and to support the next steps of your work.

01 ROLES AND RESPONSIBILITIES

02 SECURITY PLAN AND REPORTING

03 SECURITY CULTURE

04 CRISIS MANAGEMENT

Good security management

Companies & organizations

INTRODUCTION

ROLES AND RESPONSIBILITIES

01

What?

A robust and efficient security organization requires clearly defined roles and responsibilities. It must be clear across the organization who is responsible for implementing and executing security measures, such as screening new staff, and who has the mandate to make security-related decisions, for example when entering into new partnerships or collaborations.

Defining roles and responsibilities is relevant at all levels of the organization to make it clear who has the overall responsibility at management level, and who is responsible for day-to-day operations at project or department level.

Why?

By clearly defining the decision mandates, you ensure that security-related decisions are made at the appropriate management levels. Taking principal or high-risk decisions at central management level helps to ensure that security risks are assessed in a uniform manner, thereby building a shared understanding of your organization's risk acceptance.

Furthermore, clarification of responsibilities goes hand in hand with your efforts to ensure that the right qualifications required for the security task are available. Be mindful of the fact that security is a field of responsibility that requires wide-ranging qualifications, including knowledge of legal, police and social affairs.

How?

- Identify key decision-makers.
- Specify the mandate and escalation responsibilities of key decision-makers.
- Explain how different decision mandates and management positions relate to one another.
- Assess which decisions to escalate to which management level – for instance in relation to partnerships, collaborations or employment – and set uniform criteria for the escalation process in order to ensure a consistent approach across units.
- Examine whether already existing committees and management structures could be expanded to handle security-related tasks as well.
- Consider whether a coordinating committee could facilitate the implementation of security tasks across the organization.
- Assess whether the required security qualifications are available at the local level, or whether central support functions may be consulted to ensure efficient security-related work processes.
- Consider when central risk management is required, and when decisions are best handled at the local level.

Read PET's questions on roles and responsibilities, and use them in your practical work.

? QUESTIONS YOU CAN ASK YOURSELF ▶

Good security management

Companies & organizations

INTRODUCTION

ROLES AND RESPONSIBILITIES

01

Questions

Consider the following questions when formalizing roles and responsibilities:

- Who at the senior management level is responsible for the implementation of security measures? Who is responsible within the board of directors, at senior management level and at department level? How do the roles relate across different entities?
- Do you already have a security or risk committee that may handle some of these tasks?
- Is it clear at which organizational level decisions are made, for instance in relation to partnerships, collaborations, employments or outsourcing of critical functions?
- Is there a central security function with a right to veto certain decisions, for example in relation to partnerships, collaborations, employments and outsourcing?
- Are there fixed criteria for when and how to escalate specific decisions? And how to carry out and document the escalation?
- Is the responsibility for different risk types (such as cyber security and physical security) allocated to different parts of the organization? If so, is there regular cooperation or meetings between these different areas?
- Are there clear communication channels in place for the security work, thereby enabling quick and efficient clarification or decision support?
- Are there clear guidelines in place for business trips or conference participation?
- Can visitor access to production facilities etc. be granted at the local level? Who is responsible for visitor registration and handling?

BACK TO WHAT, WHY & HOW

Good security management

Companies & organizations

INTRODUCTION

SECURITY PLAN AND REPORTING

02

What?

The security plan constitutes the framework of your overall security work. This is where you specify the approach to security at your organization. The purpose of the security plan is to document the guidelines, approaches and procedures implemented by your organization. This is also where you define your overall risk tolerances. It is important to keep in mind that the security plan is a dynamic document that should be updated in response to changes in internal or external circumstances, including new information on partners or suppliers, technological developments, legislative amendments etc.

In continuation of the security plan, a key component of sound security management is to formalize regular reporting. You should ensure that the board of directors, key decision-makers and any relevant committees are regularly briefed on ongoing security work across the organization.

Why?

The security plan contributes to a shared understanding of your security and risk-related work and can be used to update staff, partners and others on the procedures to follow when working at or cooperating with your organization.

The formalized reporting helps to ensure that the relevant decision-makers are up to date on security risks across the organization. Knowledge of the overall risk picture is key to ensuring that you have a complete and up-to-date overview of your vulnerability coverage, risk assessments and ongoing mitigating measures. This provides a platform for efficient and continuous security risk management.

How?

- Formalize ongoing and future measures aimed at supporting your security work, and document these measures in a central document that will serve as your security plan.
- Include any principal decisions in your security plan, clarifying for instance if certain collaborative partnerships fall outside your risk tolerance.
- Set a fixed review cycle for the security plan, specifying when vulnerability analyses and critical technology mappings should be revisited.
- Assess if there is a need to introduce criteria for ad-hoc updates of the security plan or security reporting for example if new legislation is introduced or central technology registers are updated.
- Define which topics to report on and when. Find out who will deliver and receive the data and where to compile it. You should also decide who in the organization is responsible for complying with the individual reporting obligations.
- The regular reports may include decisions concerning ongoing partnerships, supplier agreements, outsourcing agreements, research collaborations, and so on.
- Specify a standard format for post-indicent reviews and reporting in order to ensure that such incidents are actively used as a basis for improving existing measures and introducing new ones.

Read PET's questions on security plans and briefings, and use them in your practical work.

? QUESTIONS YOU CAN ASK YOURSELF ▶

Good security management

Companies & organizations

INTRODUCTION

SECURITY PLAN AND REPORTING

02

Questions

Consider the following questions when working with security plans and reporting in your organization:

- Do you have formal guidelines for your security work (at the central level, in local departments and at production facilities)? If yes, do the guidelines at the local level match the requirements set out at the central level?
- Do you regularly update your security plans, including e.g., travel instructions, etc.? If yes, is it clearly defined who is responsible for these updates?
- How do you ensure at the local level that any updates of security plans and instructions, etc., are communicated to your staff?
- Do you have a procedure for incorporating security into new projects, partnerships, collaborations, procurement, etc.? If yes, do you know where to find it?
- Do you know how to access key security information at the local level, including risk assessments and mitigating measures in relation to employments, procurement, security incidents, etc.?
- Do you have guidelines for reporting and handling security incidents? *(See the section on crisis management).*
- Do you provide formalized reporting at regular intervals – and in a fixed format – to a central security committee and/or board? Have you specified how the reporting should be used in relation to updating guidelines?
- Do the key decisions-makers in the organization have access to an up-to-date and comprehensive risk picture?
- Is it clear to the management where in the organization different security data are processed and who is able to identify and extract data relevant for reporting purposes? (Are screenings of new staff for example registered by an HR unit at the local level?)
- Is security a permanent agenda item in connection with board meetings, central committee meetings etc.?

BACK TO WHAT, WHY & HOW ◄

Good security management

Companies & organizations

INTRODUCTION

SECURITY CULTURE

03

What?

A strong security culture helps to ensure that security remains top-of-mind in all work-related activities. Furthermore, it creates a shared understanding of the framework and ideas that characterize the approach to security adopted by your organization. Security culture in this context refers, for instance, to your handling of passwords, onboarding and offboarding procedures, and the fostering of sound and trusting communication.

Why?

Building a strong security culture contributes to security work becoming a shared task across the organization. Clear management communication – at the central and local level – emphasizes that security should be an integral part of daily activities. The aim is to form an environment where all staff feel equipped to make the right decisions and have access to the necessary support, including local guidance material. The staff should also feel comfortable seeking help and guidance from those responsible for security.

How?

- A strong security culture requires the management level to clearly communicate why security is a priority in your organization in order for everyone to grasp the importance of new measures.
- Make sure that guidance material is readily available to the staff and that procedures are communicated in a manner that clearly illustrates why it is important to follow them.
- Support local ownership to ensure that measures initiated at the central level are also adopted by departments at the local level.
- Consider how your security culture is communicated to new staff and partners in a way that makes them understand the principles and codes of conduct they are expected to observe at your organization.
- It should be easy and safe to report any incidents caused by human error. In support of this, you may consider introducing a whistle blower scheme or expanding your existing scheme.

Read PET's questions on security culture, and use them in your practical work.

? QUESTIONS YOU CAN ASK YOURSELF ▶

Good security management

Companies & organizations

INTRODUCTION

SECURITY CULTURE

03

Questions

Consider the following questions when working with security culture across your organization:

- Are there any official guidelines (such as the security plan) specifying your security culture? If so, have they been shared at the local level?
- Are the key security messages clearly understood across your organization? Do you have any local additions to these? If so, is everyone familiar with these?
- Is the importance of security and good security behaviour clearly communicated by the management at the central and local level?
- Do staff with specific security functions, such as screening, possess the qualifications required for the task?
- Are there structures in place to support knowledge sharing on key security tasks across departments?
- Do you have procedures for informing partners what a strong security culture is for you?
- Do you offer training aimed at preparing staff to undertake security-related work at your organization? If so, who is responsible for ensuring that the right individuals are trained?
- Do you have a procedure for ensuring that new staff and partners undergo and complete appropriate security training before being granted access to your premises and critical data?
- Do you have a procedure for the staff to report security incidents? If yes, is it easily accessible and widely known across your organization?
- When onboarding new staff, do you inform them about who to contact with any concerns or questions they may have?
- Does your organization have a procedure for addressing inappropriate security behaviour? If so, how is this procedure communicated to staff and partners?

BACK TO WHAT, WHY & HOW

Good security management

Companies & organizations

INTRODUCTION

CRISIS MANAGEMENT

04

What?

Crisis management is a key component of the overall security management aimed at building and enhancing the resilience of your organization. When a risk materializes or an unforeseen event turns into an actual security incident, it is important that you are ready to deal with it. Incidents can take many forms and vary both in scope and criticality, but the structures of efficient crises management remain the same.

It is also recommendable to incorporate a post-incident review process. The review should be carried out once the incident is under control and you are no longer in a state of crisis. The aim of the review is to understand how the incident occurred – and what you can do to prevent a similar incident from reoccurring.

Why?

An organization should be able to handle a security incident without shutting down all functions and daily activities. This requires careful planning across your organization as well as clear documentation and communication of the steps involved in crisis management – from identification to handling and review – to all parts of your organization.

An emergency management plan is a central element of your crisis management as it enables you to react without delay in the event of an incident. Furthermore, your guidelines must ensure clear communication throughout the process.

How?

- The emergency management plan should clearly define roles, responsibilities, decision mandates and communication channels in the event that a crisis or unforeseen incident occurs.
- Determine which functions (e.g. legal team, HR, IT, etc.) should form part of your crisis management team and who their representatives should be. You should also define who in the management has overall responsibility for crisis management.
- Some security incidents may be sensitive in nature, and it is therefore recommendable that your crisis management set-up only involves a small group of staff in order to restrict any closer examination to a limited circle.
- The roles performed in day-to-day activities should be maintained during a crisis in order to ensure that the crisis management remains attached to already established structures. This ensures that the central management along with other selected staff are familiar with the emergency management plan, their own roles as well as the crisis management principles of the organization, and that they stand ready to convene in the event of an incident.
- In all likelihood, there is already a response plan covering other types of crises, and the principles of overview, coordination, communication and restoring operations will also be relevant in connection with a security incident.
- Prepare a detailed crisis communication plan which you can use when an incident has been detected, while it is being handled, and after it has been dealt with. It is important to have considered who should know what and when. Consider both internal and external communication

Read PET's questions on crisis management, and use them in your practical work.

? QUESTIONS YOU CAN ASK YOURSELF ▶

Good security management

Companies & organizations

INTRODUCTION

CRISIS MANAGEMENT

04

Questions

Consider the following questions when working with crisis management across your organization:

- Is it clear who is in charge of handling a security incident and when to report to the different entities?
- Is it clear how and to whom a security incident should be escalated if detected at the local level?
- Do you have a permanent team with different professional profiles who are familiar with the crisis management principles of your organization and stand ready to convene? *(See the section on roles and responsibilities).*
- Is everyone familiar with the crisis management procedures of your organization? And where to find the relevant information?
- Do you have a general and updated emergency management plan comprising relevant sub-plans for handling the most likely incidents? If not, the Danish Emergency Management Agency has published a guide on how to prepare emergency management plans and risk analyses to support efficient crisis management. ***See the guide here.***
- Have you specified when to contact the authorities (including police, the Danish Emergency Management Agency, PET, CFCS, etc.), and who will do so?
- Is it possible to integrate your handling of this type of incidents with other security plans or draw on such plans?
- Do you have fixed procedures for general communication with your staff in the event of an incident?
- Does your organization have a fixed procedure for post-evaluation of security incidents, for example in the form of "lessons learned"? If so, who is responsible for this?
- Have you determined what types of incidents trigger an update of your security plan and/or emergency management plan?
- Do you have a procedure for following up on security incidents at the local level? For example, in relation to reviewing security procedures, accesses, ongoing mitigating measures, and so on.
- Have all of your staff been informed about the whistle-blower scheme at your organization and how to use it?

BACK TO WHAT, WHY & HOW ◄