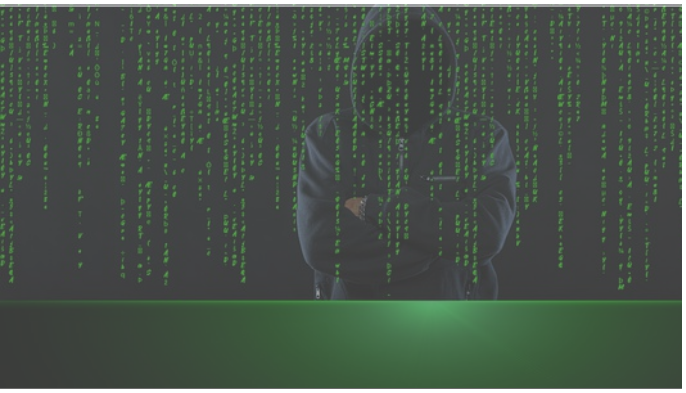
Exercise guide
Crisis team exercise
Cyber attack

controllit
Business Continuity Management

Content

Introduction



Headlines such as "Cyber Crime", "2 million customer data leaked", "Hacker attack paralyses company for weeks" can be read in the media again and again. Despite all risk-mitigating measures and company precautions, this scenario also occurs several times a year in Germany, with damages amounting to millions.

Is your company prepared for this scenario?

In this guide to a crisis management exercise (CMX) cyber attack, we want to present the essential topics for the successful handling of such a crisis.
In doing so, we pay particular attention to the classic goals of crisis management:

- **Protection of human lives**/Integrity of people and the environment
- **Damage limitation Avoidance**/minimization of economic damage, avoidance of image damage, safeguarding of (time-)critical business processes
- **Protection of normal operation** of unaffected parts of the business

Another focus is on the effective and efficient cooperation of the members of your crisis management team (CMT) on the foundation of the **basic tasks of a crisis management team**:

- Identification and analysis of crisis situations
- Determination of a strategy for crisis management
- Development of options for action
- Assessing the prospects of success, risks and opportunities
- Prioritization and decision-making
- Informing about measures taken
- Delegating and controlling actions
- Evaluation and reassessment

Preventive measures

Crisis management is a reactive process, but of course you also prepare your crisis management organisation for its tasks with preventive measures.

Here we summarize the essential measures with a perspective on the "cyber attack" scenario:

Check whether all responsible participants in your crisis organisation are capable of acting and ready for action (e.g. through regular training, meeting structure, regular exchange of information, awareness measures):

- Members of the crisis unit, including their alternates
- Participants at the tactical level (department heads, etc.)
- Implementers at the operational level (employees in the specialist departments)

Leverage your business continuity management system (BCMS) when implemented:

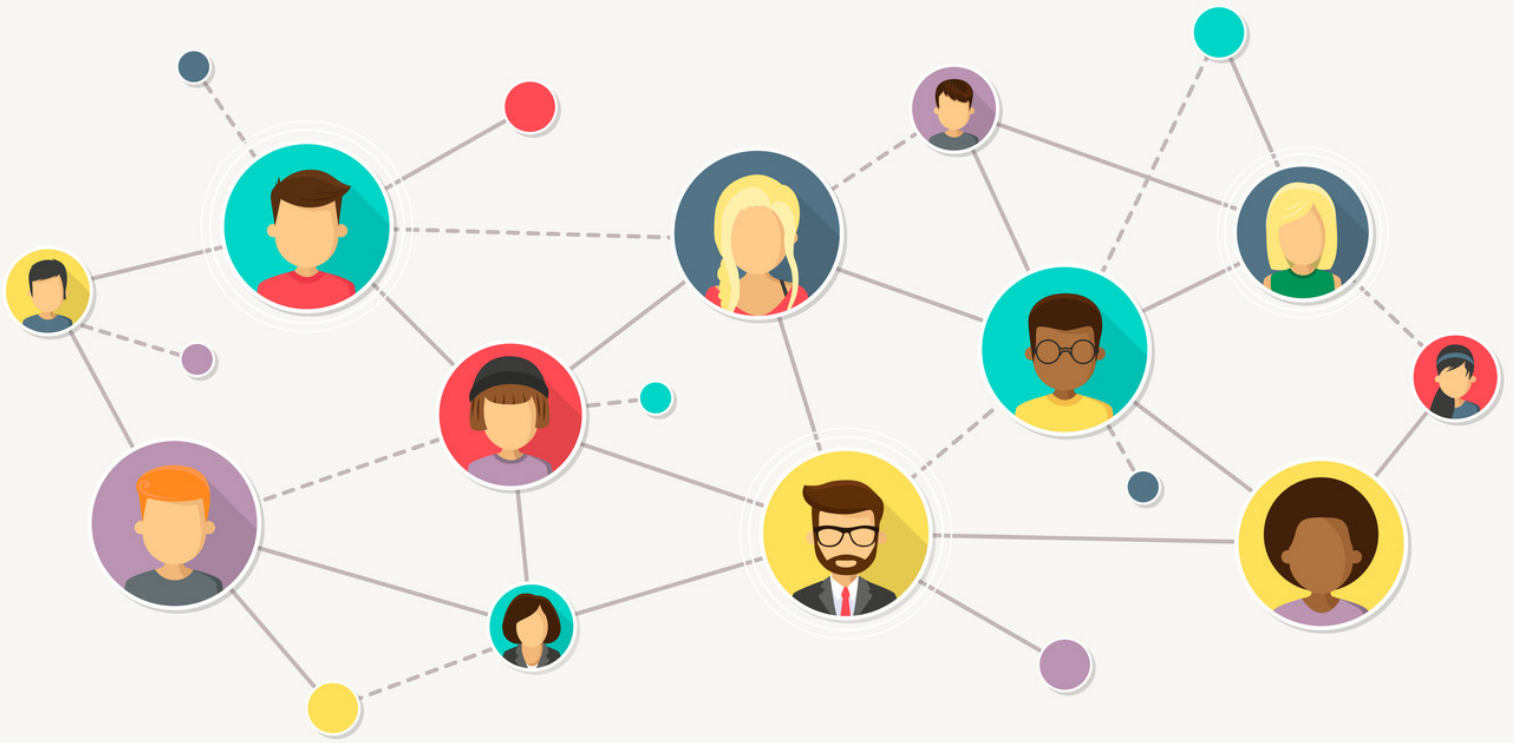
- Review the timeliness and effectiveness of business continuity plans for the IT failure scenario:
  - → In the event of an IT failure, are the solution options used able to temporarily compensate for a business process failure (especially with regard to the implemented workarounds)?
  - → Are your backup measures such as hot to cold standby etc. effective and applicable?
- If you have not implemented a BCMS, check your operational capability on the basis of the following topics

Leverage your IT service continuity management system (ITSCMS) and information security management system (ISMS) when implemented:

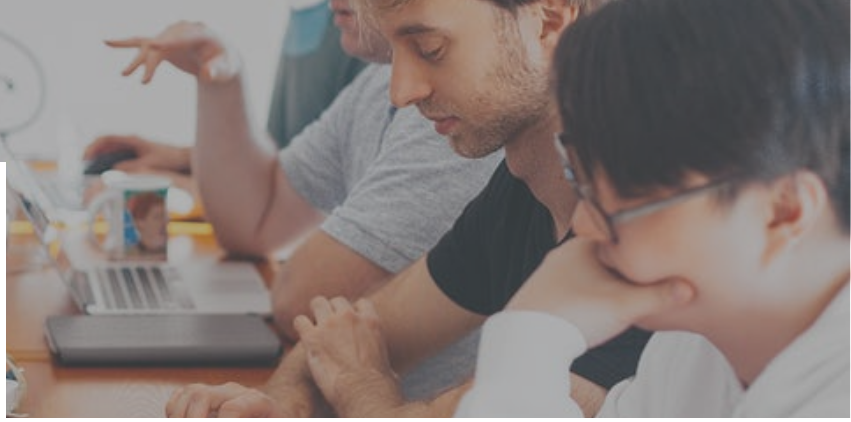
- In the event of an IT failure, are the solution options used capable of temporarily compensating for a business process failure?
- Can your IT target values such as Recovery Time Actual (RTA) and Recovery Point Actual (RPA) be met?
- Is the availability of IT services sufficiently guaranteed from the point of view of the ITSCM?
- Is resource recovery regarding an attack adequately ensured in the ITSCM?
- Are the protection objectives of the ISM adequately safeguarded?
- If you have not implemented ITSCM and/or ISM, check your readiness using the topics listed below

Preventive measures

Use the establishment and maintenance by the crisis manager of external interfaces (here in particular authorities such as the State Criminal Investigation Office, Federal Financial Supervisory Authority, Federal Office for Information Security, etc.)



Create understanding and awareness as well as procedural security for the topic (awareness measures)



Reactive measures

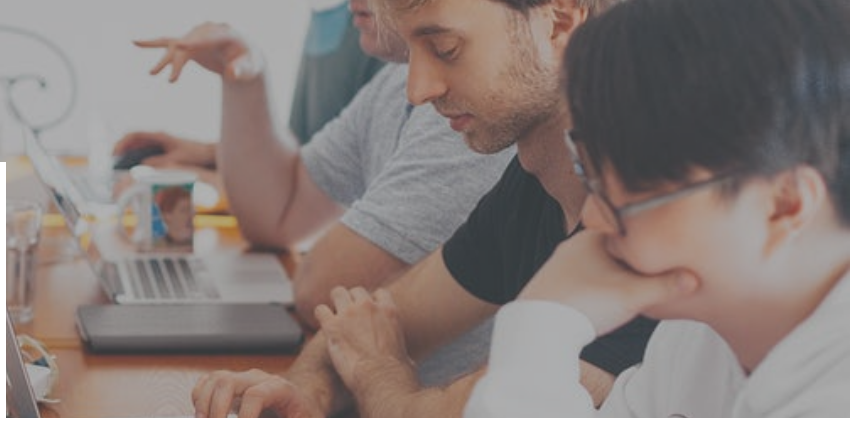
The reactive measures in the event of an incident are in the foreground in a crisis management exercise (but also in the event of the actual occurrence of the incident). This involves an orderly start to the work of your crisis team supported by a general overview of topics. The first steps as well as detailed points for individual crisis team members are presented below.

General overview of topics

In the event of a cyber attack, initial measures are initiated with the involvement of the ITSCM/ISM and, if necessary, with the involvement of external authorities: The focus is immediately on damage limitation and security measures.

In addition, the following measures and considerations are essential:

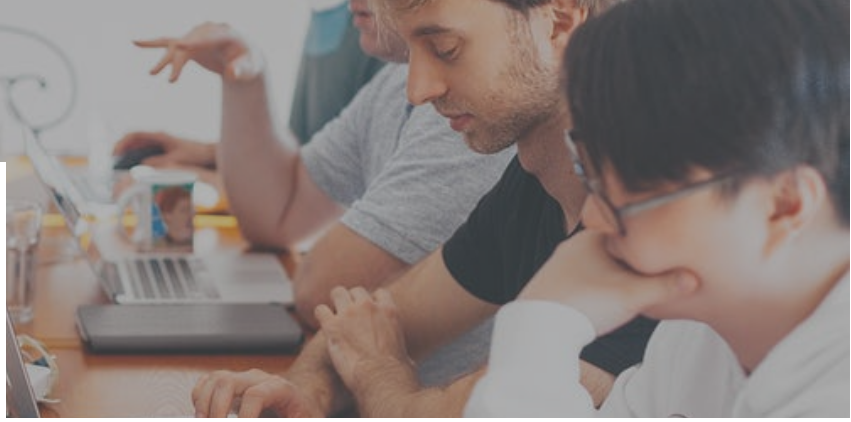
- Observe the following points when alerting and constituting the crisis management team:
  - → Crisis management room usable (possibly use of alternative CMT room)?
    - Can your crisis management room be used self-sufficiently with regard to individual or several IT components?
    - Virtual tools with connection to the enterprise system are probably not available!
  - → Identification of available IT systems and software (from telephone to website to emergency laptops)
  - → Rapid internal - external communication
    - First info: Confirmation of the event on the basis of predefined wordings (ideally within ten minutes)
    - Special attention should be paid to the positioning of the company and the external communication strategy (responsibility, perpetrator/victim, etc.)
  - → Identification and delimitation of the current and potential extent of the damage (interface ITSCM/IT)
  - → Activation of the BCPs and the IT recovery plan (if available)
  - → Obtain budget approval (if necessary)



Reactive measures

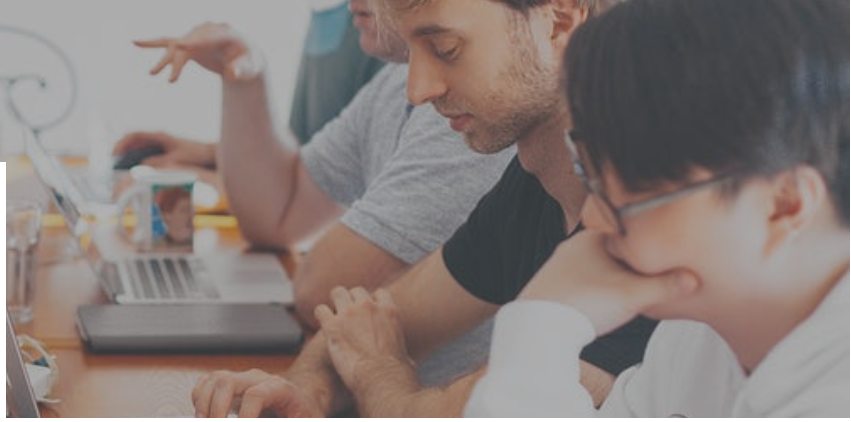
- Note a dynamic impact cascade (this is quite likely): Usually a domino effect occurs within IT systems
- Note the extremely high initial momentum and likely pressure (due to overall high IT dependency) of the chaos phase, especially in terms of information (abundance and scarcity)
- Perform the core tasks of initializing and ensuring emergency operations
- Use your organizational form: Is there an assistance and service team (AST), communication team or are members of the crisis management team (CMT) responsible for structured connection of the departments?
  - → What are the reporting and information channels?
  - → How do you integrate the interface representatives BCM, ITSCM and ISM into the CMT?
- Use the departments' connection to the AST or CMT for situation determination:
  - → Which departments are affected?
  - → Which departments are capable of working/not capable of working
  - → Which IT services are affected?
  - → Which IT services can be used?
  - → Are employees and/or customer data affected?
  - → Which safeguards are successful/can be prioritised?

- Ensure the flow of information and the coordinated connection to external interfaces (e.g. authorities such as State Criminal Investigation Office, Federal Financial Supervisory Authority, Federal Office for Information Security) as well as the timely implementation of reporting obligations:
  - → If necessary, integration of State Criminal Investigation Office or external experts (e.g. IT forensics) in crisis team
  - → Compliance with reporting deadlines in accordance with company and industry requirements



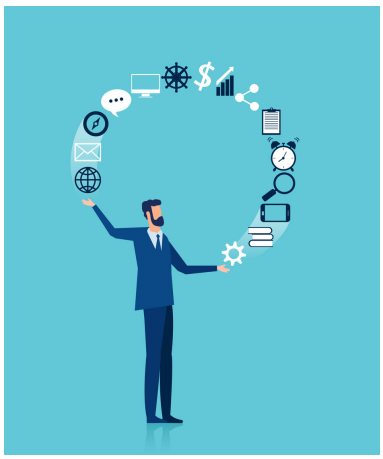
Reactive measures

- Control advanced situational awareness: use visualization for overview!
  - → Internal and external extent of damage: Which IT services are affected? Which RTA and RPA are currently realistic? Which data is affected?
  - → Which departments are affected? In particular: Which time-critical business processes and which RTO exist?
  - → Which departments are workable/not workable? Are there available business recovery options?
  - → Which IT services are needed in emergency operation and are usable/recoverable? Prioritization on the timeline?
  - → Responsibility for event: own fault/external fault/compliance with duty of care
  - → Measures overview and status control
  - → Root cause determination for optimized damage limitation (e.g. via IT forensics)
- Use your thresholds!
  - → Are thresholds defined and which thresholds are exceeded? Threshold potentially exceeded for:
    - IT failure
    - Failure IT service provider
    - If applicable, threshold values ITSCM (if available)
- Note the implications for home office and remote working
  - → VPN connections can also have an impact on employees' private devices (bring-your-own-device).
- Assess the prospect for your crisis management team
  - → In the event of an IT failure, the CMTwill probably be used for a longer period of time (depending on the type and handling of the cyber-attack)
- Start the recovery process in parallel with the emergency operation (IT recovery)
- Check your insurance cover and notification obligations (e.g. business interruption insurance)
- Pay special attention to the support of the hotlines
  - → If the telephony still works, a high additional volume is to be expected (customer and media inquiries)



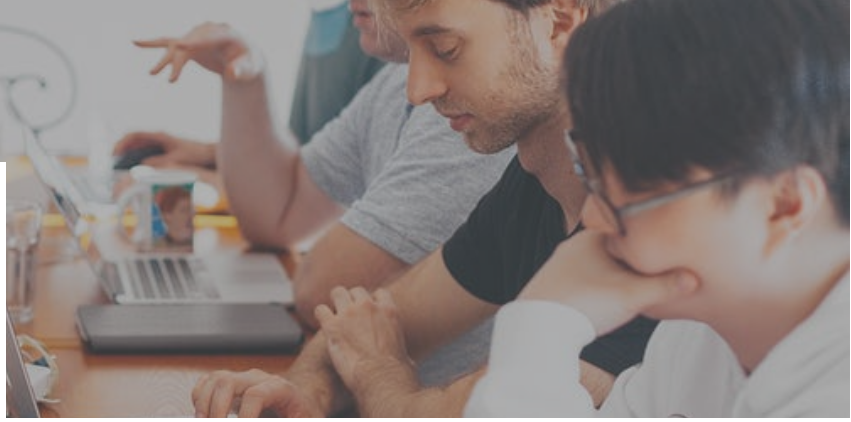
Reactive measures

Specific tasks of the members of the crisis management team



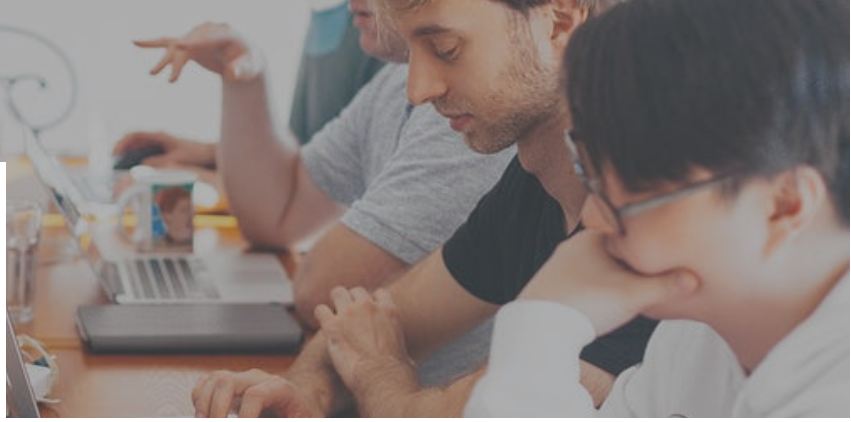
Some members of your crisis team can process their tasks according to the checklist in the "cyber attack" scenario (e.g. the function holders moderation, logbook management, visualization, assistance, legal and finance). In the following, special features of the function holders with a perspective on the "cyber attack" scenario are presented:

- **Crisis Management Team Leader:**
  - → Ensure the working capacity of the crisis management team (initial and regular)
    - Integration of relevant functions and roles
    - Availability of sufficient resources (technical, spatial, etc.)
  - → Establish a functioning framework for cooperation
    - Schedule, briefings, documentation
  - → Observe the reporting obligations in the context of the company (if necessary, cooperate with Legal Department)
  - → Actively manage the cooperation with authorities (if necessary, integration of State Criminal Investigation Office, IT forensics).
    - Integration of authority members in the crisis management team (if possible!)
  - → If required and operationally constrained: consolidate prioritization to operations and stakeholders
    - Core business/core processes
    - What is possible with which means (keyword IT availability)?
  - → Check the sensible use of experts and service providers
  - → Provide proactive information to management/Decision Making Authority (DMA) and committees
    - Coordination of information before press appearances (in cooperation with the person responsible for communication)
  - → Observe compliance with FORDEC
  - → Make sure you carry out the action control and an effectiveness check
  - → Keep an eye on the budget and financial control
  - → Actively manage information
  - → Practice active care (this scenario can also be stressful)



Reactive measures

- **Area of responsibility Communication:**
  - → Check which media are available in the current situation (initial and in the course of the crisis)
    - Use the available media (internal, external, social media)
    - Use your service providers for communication if necessary
  - → Pay attention to the consistency and reliability of your external and internal communication
    - First info: Confirmation of the event based on predefined wordings (ideally within the first ten minutes).
    - Appropriate communication strategy (perpetrator/victim, accountability, openness, etc.)
    - Prompt extension of communication to all stakeholders
    - Coordination within CMT, especially with IT regarding expected time lines (actively manage internal/external expectations)
  - → Note the high interest in accountability for the event
  - → Use and create FAQs (for internal and external needs)
    - Operate active information management with the relevant interfaces
  - → Support your hotlines (and service providers, if applicable) with wording templates to ensure consistent external communications



Reactive measures

- **Human Resources (HR) area of responsibility:**
  - → Coordinate potential staff shortages and surpluses (flexible staffing):
    - Which departments have staffing needs?
    - Which departments can provide staff?
    - What skills do employees have/need (active skills management)?
  - → Coordinate data control and access rights
  - → Ensure that personnel files are available to the CMT if required and otherwise locked (e.g. for internal offenders).
  - → Coordinate information management on the works council/staff council
  - → Advise on overtime and labor law if needed (manual workarounds for IT outages usually require more time and staff)
  - → Check payment obligations
  - → Use the resources of your service providers
  - → Coordinate staffing service requests as needed
  - → Actively manage information

- **Area of responsibility IT :**
  - → Inform your service providers (incl. data centers)
  - → Clarify the responsibilities within IT
    - Use of the IT emergency manual
  - → Research and provide an estimate of the extent of the IT failure (see above for extent of damage)
  - → Develop a forecast for the spread of damage
  - → Show options for IT timelines and recovery
    - Prioritization proposals on the part of IT
    - Please note the prioritization by the CMT
    - Observe prioritizations from the BCM/ITSCM
    - Integrate time and economic aspects (feasibility)
  - → Initiate the implementation initiative to restore IT services
  - → Identify and coordinate reasonable IT service providers/experts (incl. IT forensics)
    - for emergency operation
    - for recovery
  - → Operate active interface management with ISM, data protection officers
  - → Actively manage information

Reactive measures

- **Area of responsibility Department :**
  - → Check the extent of damage in your area
  - → Consolidate and communicate the requirements in your area (regarding IT and additional staff if necessary)
  - → Review and use your prioritizations regarding the core tasks
  - → Use and test the functionality and effectiveness of your bridging measures
  - → Use your expertise to flexibly and creatively apply solution options
  - → Actively manage information
    - Direction crisis management team
    - Cooperation with other departments

- **Area of responsibility ISM and data protection:**
  - → Check whether protection targets from the ISM are affected
  - → Check the effectiveness of ISM measures and adapt them according to needs and in compliance with the law
  - → Comply with the reporting requirements in your area of responsibility and actively manage information with the relevant authorities
  - → Actively manage interfaces to ITSCM, BCM and data protection officers
  - → Actively manage information
    - incl. consulting of the crisis management team on all ISM and data protection topics

Return to normal operation and follow-up

The return to normal operations after the active deployment of the crisis unit will require the usual planned measures:

- **Ensure return to normal operation according to your recovery process**
  - → Ensuring the basic functionality of IT services
    - Organization of the secured and perhaps not yet fully available IT services (e.g. dealing with performance, function, user restrictions)
  - → Coordinated handover of work packages to the specialist departments
  - → Organization of the processing of the backlog
  - → Orderly completion of the work of the crisis unit (including handover, information lines, safeguarding of documents and records)

- **Ensure structured follow-up or reappraisal of the events (lessons learned process/ postmortem analysis)**

Controllit AG
Kühnehöfe 20
22761 Hamburg
Germany
www.controll-it.de

Status: October 2021

Controllit is your partner for Business Continuity Management (BCM). Since our foundation we develop integrative concepts and products for Business Continuity Management, IT Service Continuity Management and Crisis Management. We help you with strategic, organizational and technical concepts to secure your business processes against threats and to provide for emergencies.
emergencies.

The contents of this document are intended to provide information on virtual crisis organization. Subsequent changes are possible. .

Photo credits: S. 4: iStock.com/alphaspirit; S. 5: iStock.com/alphaspirit; iStock.com/Maike Hildebrandt; iStock.com/tudmeak; S. 7: iStock.com/SurfUpVector; S. 9: iStock.com/Feodora Chiosea; S. 10: iStock.com/ipuwadol