Cyber Incident Communications Toolkit

Preparing for, and responding, to a cyber attack

Toolkit Contributors

Dr Paul Harness, Retired CIO

Paul was Director of Information Systems Services at Lancaster University from 2013 to 2022. Paul is a former Trustee and Vice Chair of UCISA.

Dr Jason Nurse

Dr Jason R.C. Nurse is a Senior Lecturer (Associate Professor) in Cyber Security at the University of Kent and Public Engagement Lead at the Institute of Cyber Security for Society (iCSS).

Dave Thornley

Dave is Head of Digital Architecture at Sheffield Hallam University and the current Chair of the UCISA. Security Group

Working Group members

Dr Gabriela Ahmadi-Assalemi, Deputy CISO, University of Cambridge
Pri Alagoda, Chief Information Security Officer Nottingham Trent University
Alice Oliver, Head of Internal Communications University of Derby
Emma Barwell, Head of User Experience and Engagement, ITS, University of Wolverhampton
Tessa Rogowski, Assistant Director University of Essex
Christi Hopkinson, Head of Service Operations University of the West of England
James Eaglesfield, Head of IT Governance University of Derby
Diane Montgomery, Assistant Director University of Glasgow
Ben Bull, Head of Legal & Compliance, Falmouth University
David Carson, formerly University of Glasgow
Graham Ingram, Chief Information Security Officer University of Oxford
Thomas Willson, Security Team Leader Imperial College
Alison Lochhead, Director of Corporate Communications, University of the Highlands and Islands

Executive Summary

UCISA works to enhance the collective expertise of its community through the strategic goal *to enable the professional development of individuals and enhance the collective expertise of our community.* As part of this work, the UCISA Security Group have developed this toolkit to support universities in their preparations and responses to a cyber attack.

The impact of a cyber-attack on any organisation can be catastrophic. In the most extreme cases, for example, TravelEx in 2020, the company was forced into administration after many months of disruption (https://www.infosecurity-magazine.com/news/travelex-forced-administration/). Universities have increasingly been targets of cyber-attacks resulting in significant disruption to critical activities including clearing, admissions, teaching and research. As well as operational disruption, and reputational damage, the financial impact of a cyber attack can amount to several million pounds, and data loss can lead to significant fines from the Information Commissioner.

This toolkit provides information and resources to help universities prepare for cyber incident communications response. Effective preparation is key to an effective response, reducing potential operational impact, reputational damage and financial costs. The toolkit is based on an approach developed by Knight and Nurse (A Framework for Effective Corporate Communication after Cyber Security Incidents, https://kar.kent.ac.uk/82836/1/Effective-Incident-Comms-C&S2020-Nurse-KAR.pdf).

The toolkit emphasises the importance of a collaborative approach with internal partnerships well beyond the IT organisation, as well as with suppliers and partners to the HE sector. The toolkit does not address technical controls that have been well documented by other organisations including Jisc and NCSC (see https://www.jisc.ac.uk/cyber-security and

http


ucisa connect share transform

Strategic Goal – To enable the professional development of individuals and enhance the collective expertise of our community

I have loved being a member of the DCG committee. I can say with certainty that the experience has had a direct impact on my career advancement. I have met wonderful people and done things I would never have thought possible and that is thanks to the encouragement and support UCISA provides. I will always be an avid supporter of UCISA and the value of committee membership.

Kerry Pinny, Interim Head of Academic Technology, Head of Digital Learning Environment Support & Senior Academic Technologist

We will ensure that institutional members' staff at all stages of their career have access to professional development to aid their career progression. We will develop training and skills for the future – horizon scanning to explore what our community needs. We will draw on and harness the expertise of our corporate members, collaborating and encouraging co-creation and innovation to develop products, services and support that meet the current and future needs of an ambitious education sector. We will empower our membership and lead by example.

We will achieve success by

- Creating learning pathways for professional development and career enhancement within the education sector
- Curating useful resources and content to be made available to both Institutional and Corporate members and their teams
- Exploring links with other sector bodies working with them and our membership to develop innovative progression opportunities and early career placement schemes
- Increasing the number and type of training bursaries on offer
- Ensuring our events are career enhancing and seen as offering value to members
- Targeting our investment to further these aims
- Monitoring and measuring our Progress and Member Satisfaction

UCISA continues to evolve to meet changing sector needs, establishing two new Communities of Practice (User Experience and Business Technology Standard) and a new Security Special Interest Group in the past 12 months

We will know we are successful when:

1 We have a recognised Accreditation Scheme and have established microcredentials

2 We have a well-regarded 360° mentoring scheme

3 We are recognised as the provider of platforms for peer-to-peer advice and guidance, facilitating and championing best practice (a peer-to-peer digital network)

4 Key stakeholders and suppliers actively aspire to co-creation with our members seeking out our collective expertise to provide sector insight to inform innovation

10

What's in the toolkit?

This toolkit is intended to be adapted by other institutions and includes resources to enable teams and colleagues across a university to work together effectively in case of a cyber attack.

The toolkit is likely to be of use in the following circumstances:

- Ransomware attack or similar
- Significant data loss through unauthorised access or human error
- Third Party software compromise

The toolkit includes:

- Quick start guide
- Knight and Nurse's Framework
- Pre event planning
- Cyber response flow chart
- Framing the message
- Disclosure choices
- Support from the sector including UCISA, Jisc and NCSC
- Prepare for reaction
- Delivering the message
- Adapting for your institution
- Toolkit resources

Who is the toolkit for?

The toolkit is written for higher education institutions. IT Security Professionals and IT Leadership Teams are likely to find the resource most useful but there is an expectation that it is used in close partnership with other internal and external partners including:

- Academic leadership
- Major incident response teams
- Data protection team
- Legal services
- Internal / external communications
- Student Services
- Human Resources
- Insurance / Finance
- Estates
- Key external suppliers(e.g. Microsoft, Amazon)
- Key external partners (e.g. UCISA, Jisc, OfS, UKRI)
- Insurers

Assumed Approach to Major Incidents

Institutions are likely to have variation in their approaches to major incident management procedures. For the purpose of this toolkit, it is assumed that most are based on the Command Structures published by the College of Policing: https://www.college.police.uk/app/operations/command-and-control/command-structures

This includes a Gold Silver Bronze (GSB) team approach where:

- Gold – strategic
- Silver – tactical
- Bronze – operational

In larger, federated institutions, there may be multiple layers of GSB but the overall principles apply.

The resources in this toolkit provide you with a practical way to prepare your communication plan for a cyber attack. Exactly how long your project will take, will depend on several factors:

1. Do you have the backing of your CIO/IT director and the wider university leadership team? *Getting top down and visible commitment will be essential for the success of the project.*

2. Does your university have an existing major incident response plan/approach? *If so, then you should align your cyber response plan with this process. If you cannot do this, you will need to spend more time building an organisation wide approach.*

3. Do you have an existing IT major incident response plan that covers response to a cyber attack? *During a major cyber incident you are likely to need to call on external resources from suppliers, UCISA, Jisc, the National Cyber Security Centre, the National Crime Agency and others.*

4. Who are responsible for External and Internal Communications, Data Protection and Legal Services in your organisation? *It is strongly recommended that this work is undertaken in close partnership with the team(s) responsible for communications, data protection and legal. Given the scale of implications of a cyber incident any planning and response will require close partnership working.*

Once you have answered the above questions, you can get started. The outline below assumes that you will undertake the work as a traditional IT project, but you may want to adapt this depending on how you run projects, and how much 'process' you feel you need in your organisation.

1. Identity a Project Sponsor – *this might be your CIO, or someone senior in your IT leadership team.*

2. Identify a Project Manager – *to coordinate the work*

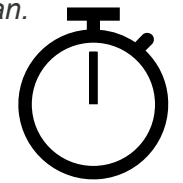
3. Identify senior suppliers to work with the Project Manager – *this should include: IT infrastructure, Information Services, IT security, Data Protection, Legal, Internal and External Communications.*

4. Identify senior users to work with the Project Manager – *this might include: senior academic user, student services, HR, Finance.*

4. Agree how you will report and monitor progress on your project – *this should be in line with your organisation's Project approach, and it is suggested that the senior team receive appropriate updates.*

5. Put in place appropriate project documentation as you require – *by answering the questions earlier in this section, you should have an idea of what your mandate it, so the next step would be to flesh out a Project Initiation Document and outline plan.*

6. Get started!



Framework for Communication after a Cyber Incident

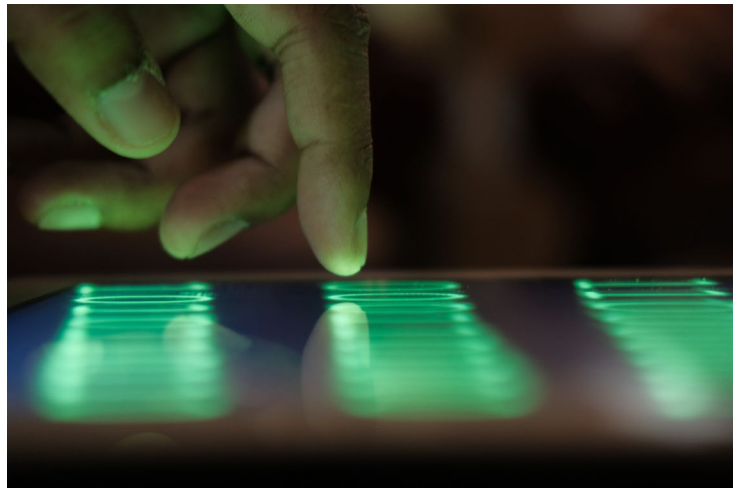
This toolkit is based on a framework developed by Knight and Nurse ”A framework for effective corporate communication after cyber security incidents” (https://doi.org/10.1016/j.cose.2020.102036). Their framework was developed from a corporate perspective and in this toolkit is contextualized for the higher education sector. The toolkit also provides supplementary resources from across the sector to help adaption on a local basis.

In an educational context, the framework is to be viewed on the basis that cyber incidents and attacks are a harsh reality faced by universities today. Effective communications following an incident form a critical element of the activities needed to protect the organisation, its students, staff and partners, and its reputation more generally.

The toolkit aims to support you in the event of a cyber security incident by providing extensive guidance on how to communicate and engage effectively in such situations. This can inform and complement existing business continuity planning practices and help increase resilience.

The toolkit focuses on the need for *preparation* providing advice on what universities should do *before* a breach occurs, as well as to help respond after a breach to reassure students, staff and partners.

The toolkit addresses questions such as: **What mechanisms should be in place to best prepare for if a security breach occurs? How should a security breach be communicated to stakeholders? When should it be communicated and by whom?** Answering these questions in the right way can make a substantial difference to how stakeholders respond to the news of a breach.



Pre-Event Planning(1)

Post Event Aims and Priorities

Effective preparation is key to minimising the impact of a cyber attack. Start by considering what your **post event aims and priorities** should be. Your list might include:

- *Protecting data subjects* – students, staff, others
- *Minimize disruption to academic activities*
- *Managing key stakeholders* – funders, enterprise partners, OfS, UCAS, others
- *Protecting recruitment* – particularly Clearing if at that time of year
- *Legal obligations* - OfS, ICO*, Jisc**, funders, contracts …
- *Internal Policies and procedures*
- *Limiting reputational damage*
- *Minimising cost of incident*

* Note specifically the requirement to report to the Information Commissioner's Office within 72 hours of identification of data exfiltration event.

** Reporting to Jisc is required by the Janet Security Policy

Crisis Communications Capability

It is assumed that you have a crisis communication capability set in the context of your major incident approach - based on a Gold/Silver/Bronze structure. You should aim to work within this and consider the following:

- *Identify decision makers* - During a cyber incident, the CIO and IT leadership/security will provide key information to a *cross functional crisis team (Silver Team)*. Who needs to be on this team? Who can chair the team with sufficient knowledge and authority?
- *Educate and support decision makers* – to ensure they are prepared and understand their roles.
- *Establish crisis information knowledgebase* - details of rules, policies, contracts and legislation for key stakeholders including any international jurisdictions you may work in.
- *Draft responses /* templates for: ICO, OfS, business partners, students, staff, media.
- *Emergency Communications* - Consider emergency website, hotline, bulk SMS, social media.
- *Ensure crisis information is accessible during an incident* – including emergency operations centre location.
- *Insurance* – ensure emergency incident and legal cover is included in relevant policy (e.g. cyber insurance, business continuity).

Pre Event Planning(2)

Partners and Supply Chain

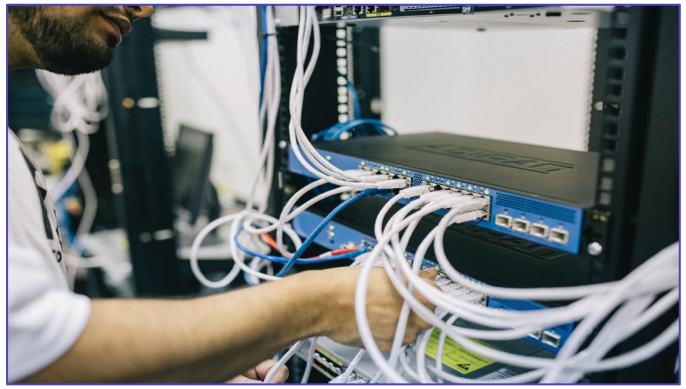
- *Suppliers - Ensure contracts with suppliers are adequately protected for breach situations.*
- *Partners – Ensure contracts where the university is the supplier account for breach situations.*
- *Involve key partners in planning and rehearsals*

Identify Security Gaps to Inform Response

You should also **pro-actively identify any security gaps you are aware of to inform the communications response**. Ensure that regular Penetration testing takes place in addition to threat monitoring, to inform you of potential vulnerabilities and enable pro-active defences to be established.

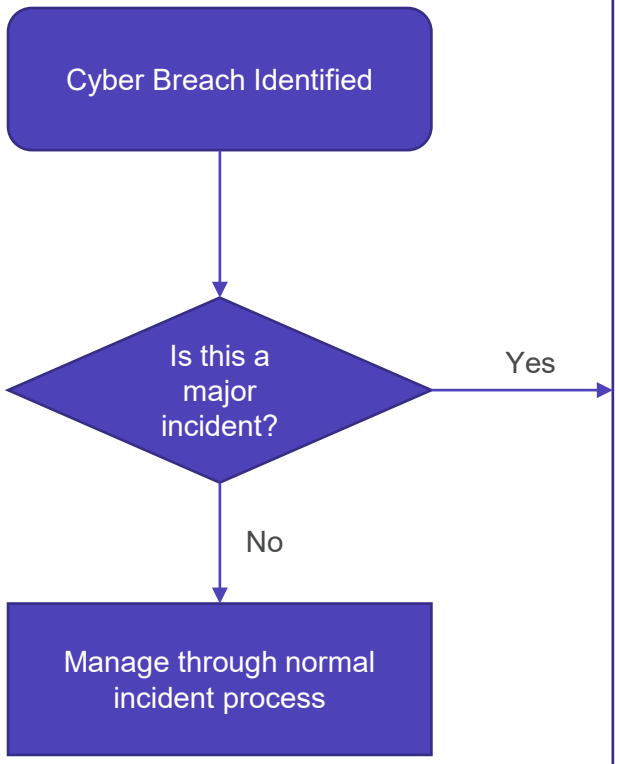
Rehearsals and Testing

- Incorporate communications response within Business Continuity Plans and Major Incident Rehearsals
- Involve key decision makers
- Work through realistic scenarios
- Include scenarios for breaches in supply chain (e.g. software and hardware providers)



Cyber Crisis Response

When a major Cyber incident occurs, there are several decisions that need to be made quickly around disclosure and communications. These are illustrated in the flow chart below and expanded further over the next few pages.



Major Incident Teams

- Gold Team - Strategic
- Silver Team - Tactical
- Bronze Teams - Operational

Disclosure?

Is disclosure mandatory?

Considerations
Who is affected?
Is the data encrypted?
How much data is lost?
Any specific rules related to, e.g. contract, legislation?
Any international aspects?

Disclose anyway?
Right thing to do?
Risk of data appearing on dark web later?
Risk of whistle blower?
Shows taking matter seriously
Reduces litigation risk

What to disclose?
Consider regulatory requirements
Consider data subject perspective
Consider media perspective

Communications

Frame the message

Accept responsibility
Avoid downplaying
Address needs of data subjects
Avoid blaming others
Consider how data subjects and media will react? Have you had any previous breaches?
Are you working with law enforcement?

Channels
Targeted email, if possible
Staff/student intranet, if possible
Website, Twitter
Formal press release?
Vice Chancellor statement?

Prepare for Reaction
Frequent internal comms
Emergency website
Call centre
Media enquiries

Disclosure

Better to notify stakeholders as quickly as possible

- Helps address feelings of vulnerability for those affected (including, for example, staff and students)
- Important data subjects hear it directly from you first to avoid a loss of trust
- May be easier to frame public opinion at an early stage in a crisis
- Obligations to OfS and others affected by the breach

Balance between accuracy and timing

- Sometimes difficult to ever establish true scale of breach
- Avoid underestimating

Based on regulations for applicable jurisdictions

- Support from internal legal team or external advisors (e.g. through insurers)
- Advice from law enforcement

How to disclose

There are pros and cons to the communications channels that may be used as follows:

- *Email* - Requires email address; May enhance perception of harm and generate negative emotions; Can be tailored to target those most impacted; Challenges include server throughput, spam filters and policy restrictions
- *University Website* - Less direct – data subjects need to visit site; Can contain FAQs, hotline nos.
- *Surface Mail* - More direct and personal; Avoids risk of phishing; May not have correct (up-to-date) address; Expensive and may also be seen as damaging to the environment
- *Telephone* - More personal / caring; Resource intensive; May not have current number
- *Social Media* - Opportunity to set the initial tone of social media posts; Interactive so able to set straight negative rumours; Risk of negative reinforcement spiral, e.g. “twitter storm”
- *Traditional Media* - Often main source of information for some stakeholders; Media typically have own agenda and may not focus on the things you want; Consider list of trusted journalists to help disseminate

It may be appropriate to use all available channels for communication to increase reach. Some channels may be disrupted as a consequence of the incident. Avoid limiting the choices of channels.

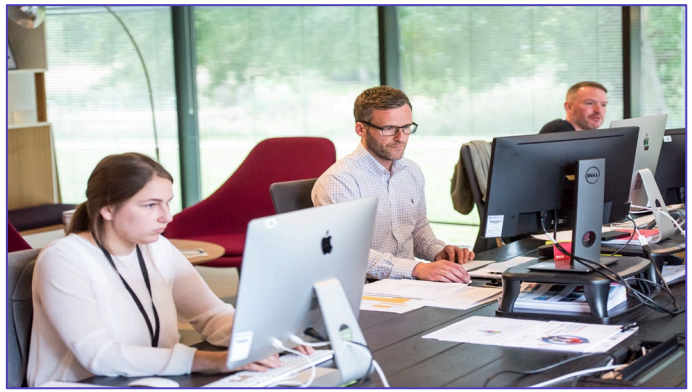
Frame the message

Guidance on Messaging

- *Accept responsibility* – you are the custodians of their data – apologise
  Even when a stakeholder is at fault (e.g. password reuse), you will be expected to have mitigated through multi-factor authentication and monitoring
- *Avoid downplaying* – may be seen as not taking breach seriously
- *Address feelings of vulnerability for data subjects* – Identify ways data subjects can protect themselves, consider providing free credit monitoring to affected students and staff
- *Avoid blaming others* – Blaming hacking groups gives them the limelight, blaming service partners can lead to public disagreements.

Considerations

- *Review aggravating factors to avoid message damaging credibility, for example:*
  - Previous data breaches – “Are you really taking security seriously?”
  - Exposure of organisational limitations – “Is your comprehensive security plan that good?”
  - Breach being discovered by third party – “Is the security of student, staff and partner data really at the heart of what you do?”
  - Is this a “sophisticated attack” or really exposing weaknesses in your systems?
- *Take into account age, gender and cultural differences*
  - Ethical Stance – Gender and age differences
  - Younger generation may be less impressed with credit monitoring as a mitigation
- *Other considerations*
  - As appropriate, how are you working with law enforcement to bring the culprits to justice?
  - Can you share lessons learnt in due course to help others avoid repeating your mistakes?



Delivering the message

In practice, the message needs to be delivered clearly in an easy-to-understand manner and avoiding jargon. It is likely to require the use of multiple channels, depending on the specific circumstances. Specifically:

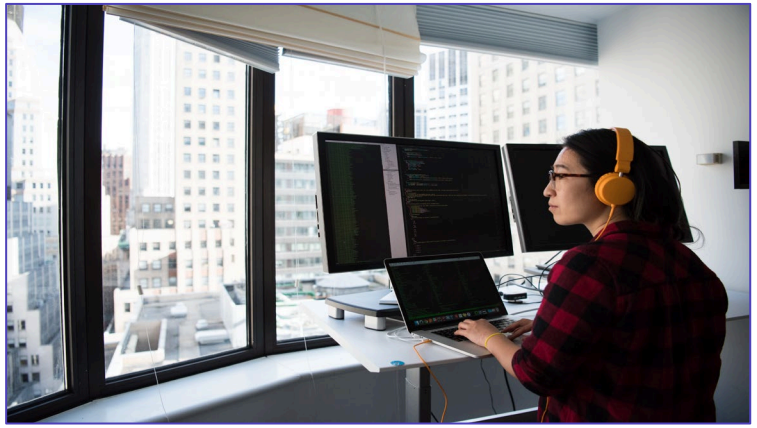
- Targeted email, if possible
- Staff/student intranet, if possible
- Statement on University Website, with links to further information
- Posting on University Twitter feed
- A formal press release
- Through UCISA to communicate to the HE IT community, particularly if other universities may be at risk

To demonstrate that the organisation is taking the incident seriously, consider who the message is sent from – in the most significant cases, this should be the Vice Chancellor.

Prepare for reaction

Once a communication is released, there is likely to be a reaction that can be anticipated. The following guidance should be followed:

- Prepare to ramp up frequency of internal communications – briefing staff including senior officers, Heads of department etc
- Ensure sufficient social media / call centre resources
- Scale up response website and telephony capacity
- Anticipate move of transactions to non-breached channels
- Ensure capability in place for dealing with media enquiries, and relevant staff training in media interviews
- Put measures in place to disrupt phishing/scam attempts as appropriate



Team Resilience

The lifecycle of a major cyber incident is generally long and complex and does not end when services are restored. There can be significant impact on staff involved in the response, and on the organisation as a whole.

During the initial stages of an incident, adrenaline runs high, and staff involved work extremely hard to get a resolution. This may require working extremely long hours, collecting of evidence for law enforcement, ensuring compliance with expectations of insurers, and dealing with a constant barrage of queries from Silver team.

This can rapidly take its toll on both staff on the ground and leadership involved in the response. It is essential that plans are in place to rest staff and provide some resilience in support teams and leadership. The impact will extend well beyond IT, as business operations are interrupted creating a backlog of work.

Post incident Activities

Once services are restored there are likely to be many ongoing tasks that, in some cases, can last several years. This can include:

- A formal report on the incident to the university's governance committees, including any lessons learned and future investments required
- Reports to external partners as appropriate – e.g. funders
- Liaison with insurers on any claims process
- Provision of evidence and witness statements to law enforcement organisations
- Working with legal advisors to deal with any claims that may result from the incident

In order to ensure that these post incident activities are as smooth as possible, it is vital that evidence is preserved, and the formal management of the incident is documented, for example, the formal minutes of meetings.

The importance of rehearsals

A vital part of the preparation process is regular rehearsal of potential scenarios through 'table-top' exercises. Such rehearsals will typically aim to:

- Evaluate effectiveness of Major Cyber Incident Response Plans;
- Gain a level of understanding of the likely impact of an incident.
- Test the proposed communications mechanisms, understanding the difficulty of crisis communications mechanisms.

The benefits of rehearsals include:

- Reduce Incident Response Times. *Re-affirm the responsibilities for decision making at different points in the incident.*
- Minimise Business Impact. *Understand the likely imposition an incident will have during an event.*
- Improve Information Flow and Trust. *Ensure that the organisation feels prepared before going into the next maximum vacation period. Mechanisms to deliver situational awareness to decision makers.*

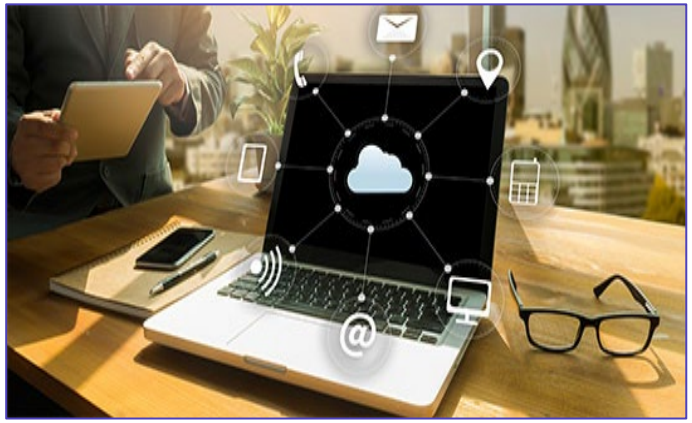
Depending on the maturity of your organisation, you may wish to consider splitting up your rehearsals into a series of shorter exercises with your Gold, Silver and Bronze teams. Whilst these will not replace the importance of a full rehearsal, they can be useful in their own right.

Rehearsal can be as much about education as testing procedures. For example, it is commonplace for business teams to assume that IT should be able to recover data – what if this turns out not to be possible?!

You may wish to approach rehearsals as follows:

- Gold team rehearsal – emphasizing that a major cyber incident is likely to have organisation wide impact, and require strategic decision making and top-level communications
- Silver team rehearsal – emphasizing the importance of effective partnerships across internal teams, and with external partners and suppliers.
- Bronze team rehearsal(s) – these may be run in different functional areas including IT (ransomware attack) and Business teams (to consider the impact of extended data loss on functional areas)

Internal audit may also be able to support and review the preparation and rehearsal processes and give appropriate assurance to Audit Committee.



Support from UCISA

During a major incident, it if often the case that focus on dealing with the matter in hand and potential support from both UCISA and Jisc can be overlooked.

UCISA

UCISA offers a confidential support service for IT leaders facing a cyber security incident. The UCISA team has excellent networks across the sector and can discreetly connect you to other IT leaders and teams who have been through similar incidents. Informal advice and support during what is likely to be a very stressful time can be invaluable. Any discussions are completely confidential, and no details will be shared without your explicit consent.

With your consent, the UCISA team can also deal with communications that may be required to all universities, for example, where other institutions may be at risk of a similar attack. This can be done without identifying your institution where necessary. UCISA also has highly effective links with key staff at Jisc.

Support from Jisc

Jisc CSIRT

Jisc's incident response team, Jisc CSIRT, monitors, coordinates and aids to resolve any security incidents experienced in the sector and has routinely supported institutions for the last 30 years to respond to or to prevent cyber attacks.

Jisc CSIRT provides proactive incident management, coordination, training, and outreach to all its members including up to date advice and guidance to help reduce threats and compromise. CSIRT liaises with partners and agencies, such as the NCSC, to provide up to date intelligence to mitigate attacks. When incidents occur, the level of support given by Jisc CSIRT will vary depending on the type and severity of the incident with special attention given to issues affecting members' essential infrastructure and business continuity.

Further information on Jisc CSIRT is available at https://www.jisc.ac.uk/csirt

Staff with responsibility for cyber security are encouraged to join the Jisc Cyber security community group for advice, guidance and to share incident information https://www.jisc.ac.uk/get-involved/cyber-security-community-group

Jisc CSIRT can be contacted at irt@jisc.ac.uk or 0300 999 2340

Support from NCSC

The National Cyber Security Centre (NCSC) works closely with the HE sector and provides extensive advice and guidance on their website https://www.ncsc.gov.uk

The NCSC also provides a free service called Early Warning (https://www.ncsc.gov.uk/information/early-warning-service) which is designed to inform your organisation of potential cyber attacks on your network, as soon as possible.

You are encouraged to report cyber incidents to the NCSC – you can do so here: https://report.ncsc.gov.uk/ The NCSC won't share details with regulators, such as the Information Commissioner's Office, without first seeking your consent.

The NCSC's Cyber Incident Response (CIR) scheme (https://www.ncsc.gov.uk/information/cir-cyber-incident-response) is designed to help you identify NCSC-assured cyber incident response providers, who will help you navigate the activities during and immediately after a cyber incident.

You may be required to notify multiple organisations as different organisations have different remits. If you are unsure who to report to, please use the Cyber Incident Signposting Service (CISS) for guidance.

The NCSC operate the Cyber Security Information Sharing Partnership (CISP) which is a joint industry and government digital service to allow UK organisations to share cyber threat information in a secure and confidential environment. Further information on CISP can be found here: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

Toolkit Resources

The toolkit is designed as a set of resources and prompts to be adapted by different institutions. Universities vary in size and complexity, and their major incident response processes are at differing levels of maturity.

It's important not to be overwhelmed by the potential breadth and complexity of cyber incident response. Resources in the toolkit are intended to be a *starting point and may be simplified or enhanced depending on your circumstances.*

Even if you consider your organisation at a low level of maturity, you can start to make improvements using the resources in this toolkit.

Start by downloading the companion file Cyber-Toolkit.zip which contains examples and resources to be adapted as required.

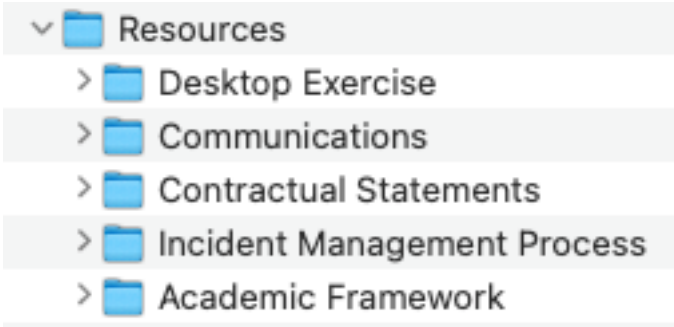
Resources include:

- Academic framework and whitepaper (Knight and Nurse)
- Communications Resources (examples from several universities including staff/student emails, social media, political and other considerations)
- Example contractual statements for suppliers and partners
- Example desktop rehearsal exercise
- Incident Management documentation

If you have resources that you would like to share with the sector, please email membership@ucisa.ac.uk to discuss having these added to the toolkit.

Copyright and Acknowledgements

UCISA would like to thank the contributors of material in this toolkit which comes from several sources across the sector and from Jisc and NCSC. Accompanying resources associated with this toolkit are © for the university/organisation that produced them and maybe adapted for use by other UK universities under CC-BY-NC. The resources may not be used for commercial or other purposes without written permission from the relevant university/organisation. Specific information is provided in each resource within the ZIP file.



Follow on activities

The Cyber threat is something that is continually changing and UCISA sees this toolkit as something that will evolve over time to continually support the HE community. You can help by doing the following:

Transparency

It generally helps to whole community to share as much information about any incidents as you are able to. For example, the Irish Health Service Executive (HSE) published a lot of detail about their experience of a ransomware attack https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf

Both UCISA and Jisc are able to help with communications to the broader sector through briefings, reports, closed Teams meetings or at their various conferences and events.

Contributions to future versions of this Toolkit

If you have resources that you think will be of use to the rest of the sector, please do get in touch with UCISA to share these. Suitable resources will be added to future versions to help it stay current and relevant.

UCISA
Registered office - 30 St Giles, Oxford OX1 3LE

www.ucisa.ac.uk

ceo@ucisa.ac.uk
membership@ucisa.ac.uk
admin@ucisa.ac.uk
events@ucisa.ac.uk
accounts@ucisa.ac.uk

Registered Company No. 09349804