**CYBERYOUTH**

**Nonformal education for cyber-security training & resilience of youth organisations and young people**

***Cybersecurity online youth academy***

****

**Policies and Procedures for Incident Response**

Table of contents

[Introduction](#_heading=h.fpb3yt6tcffi)

[It could have happened to you…](#_heading=h.c7zxm1r80lor)

[What you will learn](#_heading=h.bd1t10x6k115)

[Why it is important](#_heading=h.1fqj6c1n3ygs)

[How it can help you in everyday life](#_heading=h.bddh90wxykhs)

[What career you can pursue](#_heading=h.l25siuf1d90q)

[Pre-requisites](#_heading=h.obikvf4haym5)

[Material](#_heading=h.snpqznqbwxs)

[5.1 Organisational Security Assessment](#_heading=h.2yz7x8bu8zb5)

[Self-Evaluation](#_heading=h.nfq2guswx59)

[External consultation](#_heading=h.qycpsfx2oc3y)

[Knowing Your Weaknesses](#_heading=h.ilmmnwqn61ww)

[Prevention Tactics](#_heading=h.lzulet6qo51l)

[Conclusions](#_heading=h.q7y4utybp22l)

[5.2 Policies and Procedures for Incident Response](#_heading=h.wv8lmqsplpdd)

[Damage Mitigation](#_heading=h.se3v82rotiu3)

[Data Protection](#_heading=h.xa9iyn2x8esy)

[Prevention of Further Incidents](#_heading=h.3uw9tlbm0qe0)

[Conclusions](#_heading=h.jn7khpgf6mc9)

[5.3 Data investigation](#_heading=h.g98km9urykdd)

[Organisational Investigation](#_heading=h.d7j3sia9a2ue)

[External Investigation](#_heading=h.4rgr0sqkydi2)

[What to Look For](#_heading=h.uu16mwe9cyzf)

[Conclusions](#_heading=h.ostdn54761l3)

[5.4 Mitigation Techniques](#_heading=h.7pii0khen2cd)

[Isolation](#_heading=h.byj2zirdlb0u)

[Containment](#_heading=h.orqrn6qc565u)

[Segmentation](#_heading=h.pr0uebiv6hju)

[Conclusions](#_heading=h.8fgh3pvuc4s3)

[5.5 Digital Forensics](#_heading=h.azw51npc11fy)

[Main Aspects](#_heading=h.ucvhdpx4godb)

[The 4 Phases of Digital Forensics](#_heading=h.rpetdaosatfp)

[Collection](#_heading=h.ureo4tm4v2uf)

[Examination](#_heading=h.e3rsgig0mbwl)

[Analysis](#_heading=h.h1zlr3q64b6h)

[Reporting](#_heading=h.33k06le0uda3)

[Conclusions](#_heading=h.scbfee5behhv)

[The Geek’s Corner](#_heading=h.floxyjcfjlz3)

[Conclusions](#_heading=h.umqq3lf4f2yk)

[Quiz](#_heading=h.35btfg6prjdy)

[References](#_heading=h.ioedg3ublhq7)

#

# **Introduction**

## **It could have happened to you…**

In May 2022, Cisco, a multinational digital communications company, became aware of an attacker within their network. Their internal investigation showed that the attacker conducted a series of sophisticated voice phishing attacks to access a Cisco employee’s Google account. Since the employee’s credentials were synchronised in a browser, the attacker could easily access Cisco’s internal systems. After getting initial access, the attacker tried to stay in Cisco’s network as long as possible and increase their level of access. However, Cisco’s security team successfully removed the attacker from the network. Later on, ransomware gang Yanluowang posted leaked files on their website. According to Cisco, this breach had no impact on their business operations.

In incidents like this, response policy is the key, as you can see from the fact Cisco reacted quickly and were able to resolve the issue and avoid a disaster. It’s almost impossible to *never* suffer an attack, but it is very possible to avoid serious consequences by having a strict response policy!

Origin:<https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches>

## **What you will learn**

This module will cover a wide range of subjects in the topic of Incident Response, with a main focus on the policies and procedures an organisation can implement to improve their reaction to any potential or already occurred breaches and attacks, such as detection and information collection tools, data investigation and techniques to mitigate damages caused by an attack, as well as key points of digital forensics to learn and improve from potential incidents.

## **Why it is important**

This module is essential to further understanding how to prevent and avoid incidences, as well as understanding how to react to any possible attacks or breaches. Cybersecurity incidents don’t just disappear once they have happened, many are designed to infiltrate a network and stay until they are dealt with in the appropriate manner. By understanding Policies and Procedures for Incident Response, you can improve your capabilities in reacting to incidents and attacks, as well as develop a strong knowledge on how to identify possible incidents beforehand and avoid them entirely. Policies and Procedures are a very broad and important part of cybersecurity and ensuring the safety of your organisation, and include a very wide range of topics, all the way from network reconnaissance and detection, to recovering lost or damaged data and information.

## **How it can help you in everyday life**

The material discussed in this model aims to offer a learning experience that won’t just prepare you in the field of cybersecurity incident response, but also show valuable preparation and reaction skills that can be transferred to many facets of everyday life. With ever-increasing digital connection between all of us, incidents are becoming more common every day, which means the need to have a policy and procedure to respond to and avoid them is also becoming more important each day. This is true of both organisational security, and of everyday digital life, as the threats of cybercrimes don’t just affect businesses or organisations; we have to be careful too.

## **What career you can pursue**

After completing this module, you will have gained a foundational understanding of the fundamentals of cybersecurity. This knowledge will provide you with a starting point to explore various careers in the cybersecurity industry. Some potential entry-level career paths include:

* Cyber Security Specialists
* IT Auditor
* Infrastructure Officer
* Incident Response Leader

## **Pre-requisites**

All the modules of our course will offer valuable information in isolation, but we would encourage completing the *previous 4 modules* before taking on this module, as they are designed to be realised in order and each module will offer you more insight into the next by providing you with knowledge and situational context.

#

#

#

# **Material**

## **5.1 Organisational Security Assessment**

In the modern world, having proper security measures in any organisation is key to the safety of users, as well as members of an organisation. To keep these security measures up to the highest standard, we need to understand how to assess and check for possible issues in an organisation’s security. Understanding how to assess organisational cybersecurity policies and procedures is key to preventing, reacting to and mitigating any cyber-attacks or breaches. By assessing and understanding the weaknesses or blind spots in our organisation, we turn them into strengths by implementing policies and frameworks that take them into account and protect these weaknesses.

### Self-Evaluation

The first step to take in assessing security is to realise an internal evaluation. A key point in self-evaluating is making sure we understand what we are looking for, as well as common mistakes and weaknesses. For this reason, it is always best to involve trained various team members from IT and security backgrounds, to offer differing but informed perspectives.

The process of self-evaluating an organisation’s security can be as light or extensive as desired, but it is always best to complete a full check of any possible weaknesses, not only on the digital and technological side, but also on the human side, making sure all members of an organisation are well-prepared and understand procedures and security strategies in the organisation.

### External **consultation**

As well as a self-evaluation, it can often be beneficial to be assessed by an external organisation specialised in cybersecurity and organisational safety. Oftentimes a new set of eyes can spot things we might have missed! Many cybersecurity firms will offer an inspection or consultation service as part of their business, with many even offering to fully run your cybersecurity and safety programme.

### **Knowing Your Weaknesses**

The objective of a security assessment, whether it is internal or external, is to understand the cybersecurity situation of your organisation, as well as to help understand possible weaknesses or vulnerabilities, to know where attacks or breaches may happen, and to help develop a prevention plan, as well as an incident response policy in the case of a breach or attack.

### **Prevention Tactics**

Though not directly linked to incident response, a prevention plan with detailed tactics is highly related to the idea of incident response, as having a developed prevention plan can help develop an incident response plan taking into account the methodologies already being used in the prevention plan.

Common prevention tactics, and therefore common cases of incidents that require a response plan, can be concepts such as:

* Multi-Factor Authentication: This ensures the person accessing is the person who is supposed to access. MFA is one of the leading methods of incident prevention, but does not guarantee safety in cases such as theft of property or unauthorised entrance to a building or location.
* Access Control: Tactics such as keycards, RFID badges, etc. These are a good option for smaller teams, but can quickly become hard to track in the case of a larger team, meaning theft or loss can happen without the security team noticing.

These prevention tactics help avoid incidents, and can also be implemented as a guideline to the development of a robust incident response plan by taking into account the common breaches these tactics can suffer and guide the creation of a response to each.

### **Conclusions**

One of the keys to knowing how to keep an organisation safe is through knowing where possible threats or attacks could come from. Regular security assessments are a benefit to the organisation’s safety as conditions can change, therefore rendering security redundant or useless against possible attacks. As well as being prepared to prevent attacks, through regular and thorough security assessments, organisations can better understand how to resolve issues if an attack or incident were to happen, highlighting the importance of the proper assessment of your organisation’s cybersecurity context and situation.

## **5.2 Policies and Procedures for Incident Response**

No matter how much we prepare, the likeliness of suffering a cybersecurity incident is very likely, especially in the modern digital world. Studies showed that 80% of companies have suffered some form of cybersecurity incident during operation, which means that prevention is the best method, but, what should we do if something happens despite our best efforts?

In cases like this, it’s important to have a plan. By having a procedure to follow in case of an incident, an organisation can avoid leaving important security decisions to a single member or employee, offering them the support and tools necessary to remain safe and the framework with which to solve any possible breaches or issues. Having an incident response policy isn’t just for the safety of the organisation and its data, but also for the safety of its members and/or employees, as by providing clear and strict frameworks and steps in case of an incident, the organisation is therefore protecting them from having to make potentially unsafe or dangerous decisions, be those digital or otherwise.

### **Damage Mitigation**

One of the key points in any response plan must be to reduce the damage caused by an attack or incident. If an incident is to happen, the first step once we evaluate the damage is to reduce this, as well as limiting the effect it can have on the workings of the organisation. Data and safety are the main concerns in an incident, but another form of damage caused by breaches or cybersecurity issues is a loss of productivity due to unavailable services or data that the organisation may need in daily use.

Some of the key factors in mitigating damage from an attack or breach can be actions such as:

* If the breach or attack happened due to malware, make sure this cannot spread to other members or devices, by using mitigation techniques (discussed later on points 5.4)
* In case of any passwords or security keys being affected by the breach, re-generate the keys and/or change the passwords immediately. Even if no attempt to use these is made, it could happen at any time and the procedure to change them is a minimal effort to keep data safe.
* In case of a physical breach (unauthorised person or device) locate the breach and apply similar mitigation techniques to the affected area.
* Leave decision making to the assigned security/safety officer. It is always best to have a qualified person making potentially dangerous or high-pressure decisions.
* If it is deemed necessary by the security officer, contact law enforcement or police authorities. The most important part of damage mitigation is the safety of employees and/or team members.

### **Data Protection**

In most cybersecurity breaches, the target is the organisation’s data. This could be employee data, customer data, or even sensitive private data of underage users in the case of many youth organisations. This is why protecting this data is of the utmost importance in any case; but protection can mean various things. We have to protect the data from being stolen and ensure others can’t access it, but also need to make sure it is safe in case of deletion, corruption or any unforeseen physical incidents.

In terms of theft or attack-facing protection, some of the key factors in keeping our data safe can be methods such as:

* **The encryption of all data:** Ideally, all data we deal with should be encrypted to keep it safe from attackers. We have discussed encryption in other modules, so we’re familiar with methods and their effectiveness, but in spite of efficiency, any encryption is better than none!
* **Separation of data:** In the same vein as encrypting our data, organisations should always try and maintain separation in the data being handled, ie. Accounting data should be kept in a separate encrypted folder to User or Employee data, which leads us to our next point.
* **Access control:** Another key point in keeping data safe is making sure access to it is controlled. Data should only be strictly accessible to team members or employees who need access to it. Not only is it unnecessary for a team member in the Accounting department to be able to access passwords and information only relevant to the IT department, and vice versa, it is also an addition of an extra possible point of attack for a breach. If George, an accountant for our organisation, is attacked and a hacker gains access to his device, it is a lot safer that the hacker can only access the Accounting folder, than if they can access every piece of data available to the organisation.

In terms of data integrity and ensuring that an incident or unforeseen circumstance doesn’t mean a total loss, some important actions to take are:

* **Regular backups and restoration of all data.** These backups should be encrypted also, as well as stored on the cloud, or even in a local drive off-site.
* **Follow the 3-2-1 method: 3** copies of data, in **2** different media formats, with at least **1** being kept off-site.

### **Prevention of Further Incidents**

Now we’ve looked at how to keep our data safe and mitigate damage in case of an attack, another key point in Incident Response is the prevention of further incidents and attacks. In the case of an attack, an effective way to ensure no recurrence is to trace the causes of the breach or incident and implement a solution to the particular issue. As a general rule to follow, after suffering an incident, organisations should follow a similar procedure as when investigating for prevention, with the added context of the occurred attack in mind. As well as a general check and audit into the cybersecurity situation of the organisation, it is recommended to offer extra training to those members interested, offering resources and workshops to ensure everyone has up to date information and context. This is especially true for the initial victim of the attack, who should be offered training without being made to feel lesser for making the mistake in the first place. Just to recap, the key points in the prevention of further incidents after an attack are:

* **Troubleshooting on causing factors of the incident**
* **Organisation-Wide detailed security revision and check**
* **Further training and preparation of employees for more cyber-resilience**
* **Training of victim of attack (if applicable)**

### **Conclusions**

In conclusion, the most important steps in developing a procedure for incident response is setting correct and appropriate boundaries and roles before an incident can happen, as many of the points that will prevent further damage or issue during a breach are the same points emphasised in much of cybersecurity and security in general. We must always keep the safety of data and employees in mind when drafting a policy, making it as clear and concise as possible to ensure no errors in implementing it.

## **5.3 Data investigation**

After suffering an incident, an important part of response is understanding. Without understanding what happened and why, how can we solve an issue? With this in mind, investigation of data is key in understanding the how and why of an attack. Let’s take a look at some of the main factors in investigating an attack or breach.

### **Organisational Investigation**

The most important, and primary investigation of an incident should be the investigation realised internally, by the organisation’s IT/cybersecurity specialists, to better understand the context of the incident and how to solve it. Some of the main steps to take in cases such as these are:

* If the breach is from an unknown source or cause, check logs for the affected devices or main server, depending on the effects of the breach.
* If the source and/or cause is already known, analyse how the attack happened and the workings of the software used for the attack. It is important to understand the differences as the response to Ransomware is very different to a Man in the Middle attack, thus should be treated as very different incidents.
* If it is suspected that the attack came through from an unsupervised person or device on the network, network mapping or tracking software such as Wireshark can also be useful in finding the source of the attack.

Beyond the technical investigation, it is also important to investigate members and employees. No, don’t worry, we don’t have to interrogate them! By investigate, we mean a brief workstation check to see whether they may have also been affected, as well as inquiring into their compliance with the organisation’s policies to make sure they understand the key security measures being implemented. By doing this, we facilitate a better understanding to all team members and employees, from the victims, to the investigation team, all the way to possible other victims.

### **External Investigation**

More often than not, we will be able to investigate all incidents internally and resolve the issues without external assistance, but in some cases, especially in NGOs, or youth organisations, we may need the assistance of a specialised cybersecurity or data protection firm to resolve our issue, especially if the source of the attack is unknown to us and the attack is a recurring type (an attack that stops productivity or prevents the organisation from being able to work can be a serious issue, especially when not resolved as soon as possible). For this, we have various options:

* **Contact non-emergency law enforcement to report the crime and request assistance and an investigation:** Due to the digital nature, many people don’t take into account that cybercrimes are just that: crimes! Law enforcement agents should be able to assist you, and in many cities and locations, even have dedicated cybersecurity departments.
* **Request help from external specialists:** If law enforcement can’t help you, another effective option is to seek out cybersecurity firms near you or that may be able to assist your organisation in the resolution of issues. The obstacle for this kind of consultation in many organisations is financial, so this isn’t always an option, but more of a “last solution” if the police cannot help with the issue.

### **What to Look For**

In most cases, in an incident response context, we should be looking for anything “strange”, or out of the ordinary routine and procedure. This could be anything from a strange email an employee received, all the way to a more extreme attack such as a man in the middle attack taking control of our network, found by mapping the network and checking all devices.

There is no single thing to look for universally in an incident response investigation, hence the need for trained staff with the knowledge to investigate and who know what to expect. The amount of variables in any digital operation is too high to note a single key to look for. This is why it is important for internal investigations to recollect and understand the processes going on in an organisation to then spot the outlier or variation.

### **Conclusions**

To sum up this section, an investigation into all the information regarding an attack or breach is key to solving it. If the investigation is unfruitful, the attack could persist or reoccur and affect the organisation at an even deeper level. In most cases, an internal investigation is preferred, but many times, it is important to contact law enforcement and notify them if any serious crimes may have been committed, or especially, if any people are in danger.

## **5.4 Mitigation Techniques**

One of the keys to in-the-moment incident response (and, as discussed before, damage reduction) is mitigating the attack while it is occurring. The idea behind this is to prevent the attack spreading to other devices and causing an even bigger issue than it initially does. There are a few main methods of mitigation, so let’s take a look!

### **Isolation**

Isolation is an extreme but quick way to ensure malware of any kind can’t spread to other devices on the network, or connected in any way. Standard procedure for isolation would entail disconnecting the affected device completely from the network to cut off contact with other devices and make sure it cannot spread the malware affecting it to other machines, or even our main server. We can think of isolation as preventing a sick person from spreading their disease to other people by keeping them separate.

### **Containment**

Containment can be similar to isolation, but offers a more complex range of responses. It can range from isolating and shutting down a system, but oftentimes is seen more as controlling access or control of certain systems to prevent the attack from spreading. If isolation is separating someone to make sure no one else gets sick, containment is more so like changing the locks to your house if your keys get stolen. Many times, containment can be seen as preferable to isolation, as through access control we don’t have to incapacitate the affected machine or device.

### Segmentation

Unlike containment or isolation, segmentation aims to mitigate damage from an attack *before* an incident even occurs. In this way, it’s more of a predictive method of damage mitigation, but also will often be combined with other methods if an incident is suffered. Segmentation follows the principles of making “clusters” from VLANs, or other methods, segmenting an organisation’s network into smaller, more manageable networks, allowing them to be treated differently in terms of access control, points of access, and mitigating any possible damage to one cluster preventing it from spreading to others. In that sense, isolation is often employed if a cluster suffers an attack to prevent the other members of the cluster becoming infected with malware.

###

### **Conclusions**

To sum up how we mitigate damage in case of an attack, if we wanted to declare an order in which to employ these methods, we would perhaps go from Segmentation, looking ahead to *in case* we suffer an attack, and then to Containment, limiting damage if we suffer an incident. If these two methods don’t keep us safe, then Isolation would be the best way to proceed until the issue is resolved to ensure others are not affected by the attack or breach.

## **5.5 Digital Forensics**

### **Main Aspects**

We’ve talked about Data Investigation and recollection of information, but do we know the procedure to investigate? Digital Forensics offers a framework within which we can investigate and report on any cybersecurity issues suffered, or possibly even getting ahead of issues by finding them before an attacker does. In this way, Digital Forensics give us a method to follow in investigating to make sure we cover all our bases.

### **The 4 Phases of Digital Forensics**

#### Collection

Collect and secure digital evidence from devices like computers and smartphones using proper techniques to maintain its integrity.

#### Examination

Examine the evidence using forensic tools to recover deleted files, analyze system logs, and reconstruct user activities to find relevant information.

#### Analysis

Analyse the information we have acquired through our recollection and find a possible resolution to the found issue, through policy change or technical reworking

#### Reporting

Draft and develop detailed documentation regarding the investigation, both to present as solution and to keep documentation of the procedure and incorporate any findings into the organisation’s safety procedures and policies.

### **Conclusions**

Digital Forensics are a key part of any investigation and/or incident response, to allow a solution to an issue and also prevent reocurrence of an attack or incident. By following the 4 phases, we can gather information that will allow us to formulate a plan for the occurred incident as well as help strategize for the future.

## **The Geek’s Corner**

For those interested, here are a list of some popular Incident Response Toolkits and their features:

* [Cynet](https://www.cynet.com/partners/cynet-for-incident-responders/) : An all-encompassing package that allows administrators to get a wide view of their system and understand and further resolve incidents or attacks. Cynet also provides a 24/7 team to assist in incident response.
* Cyphon: [Cyphon](https://www.cyphon.io) provides analysts with tools to collect, process, and triage incidents. It collects data from sources such as message logs, APIs, and email—and makes it simple to analyze while allowing you to collect as much or little data as you need.
* GRR Rapid Response: [GRR](https://grr-doc.readthedocs.io/en/v3.3.0/what-is-grr.html) is Google’s framework that allows analysts to conduct remote live forensics. It also helps IR teams respond in a swift and scalable manner for faster triage and remote analysis. It comprises two parts: the GRR client, which is deployed on the system to be investigated, and the GRR server, which helps analysts implement actions and process the data they have collected.
* TheHive: [TheHive Project](https://thehive-project.org/) is a free open-source IR platform that allows multiple analysts to work simultaneously on incident investigations. It gives analysts the ability to set up notifications for new task assignments and to preview new events and alerts with multiple sources, such as email digests and SIEM alerts. Built-in templates allow analysts to gain key insights and identify the right measures to take for faster remediation.

Toolkits and frameworks such as these are a great start in being prepared for any incident or attack that may come our way. There are many other options and tools, and these are just a few. Do you know of any more?

# **Conclusions**

The key to any incident or attack is preparation. If we have a defined policy *before* an attack, we limit the damage an incident can do to our system. By defining, understanding and implementing an incident response procedure, we ensure our team is in the loop on what to do if the worst happens. After all, no matter how much we prepare, something can always go wrong unexpectedly!

## **Quiz**

**Is an incident response plan necessary if we have very strong security?**

a) No, we won’t get attacked with good security.

b) Not really, we can have one if we want but don’t need it.

c) Yes, but only for specific incidents

d) Yes, we should always have an incident response policy, as this is part of a strong cybersecurity system.

**What are the 4 phases of Digital Forensics?**

a) Collection, Examination, Analysis and Reporting

b) Collection, Deletion, Analysis and Disposal

c) Examination, Reporting, Repair and Solution-Finding

d) Deletion, Recovery, Reestablishment and Reporting

**Which of these is *not* a mitigation technique?**

a) Deactivation

b) Segmentation

c) Containment

d) Isolation

**An incident response policy aims to not only mitigate damage, but also prevent further incidents**

a) True

b) False

**What is the term for a type of cyber attack where an attacker intercepts communication between two parties in order to steal sensitive information?**

a) Man-in-the-Middle (MitM) attack

b) Cross-Site Scripting (XSS) attack

c) Cross-Site Request Forgery (CSRF) attack

d) Ransomware attack

## **References**

United States Securities and Exchange Commission. (2018). Equifax Inc. Form 8-K: Current report filing (Amended). Retrieved from https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm