



Cyber MSME








Cybersecurity for Micro, Small & Medium Enterprises

Crisis management – they hacked me, what next?

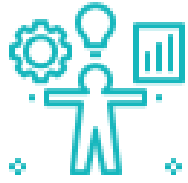
By CTS Customized Training Solutions & CASE

Objectives and Goals:

At the end of this module you will be able to:

-  identify cyber crisis in your business
-  identify potential risks and gaps
-  avoid most common cyber crisis mistakes
-  improve or create your cyber crisis management plan
-  prepare yourself for the cyber crisis response and to recovery after the cyber crisis





Unit 1: Cyber crisis management

Section 1.1: Why do you need cyber crisis management?

Section 1.2: Identify the crisis



Unit 2: Response to the cyber crisis

Section 2.1: The role of time

- The most common cyber crisis mistakes in MSME
- Why do you need a person(s) responsible for cyber crisis response?
- Cyber crisis response person's responsibilities

Section 2.2: The backup plan

- Know your providers
- Follow the traces
- Pull out the plug!

Section 2.3: Cyber crisis communication protocol

- How to speak about the cyber crisis?



Unit 3: Recovery after the cyber crisis

Section 3.1: How to return to normal after the cyber crisis?

Section 3.2: Do the assessment!

Section 3.3: Lesson learned

Section 3.4: Plan the improvements

Section 3.5: Cyber crisis case study

- Marriott International
- Lesson learned for you

Section 3.6: Summary



Unit 1: Cyber crisis management

Section 1.1: Why do you need cyber crisis management?

If you manage a micro or small business, you probably don't have enough resources and people to prevent and fight cyber crimes. For medium enterprises, it is more realistic to delegate a few specialists to work on cyber security. However, even the smallest business should feel obliged to improve cyber crisis management procedures.

Cyber crisis management protocols consist of 3 stages: 1) prevention, 2) **response to the crisis**, and, finally, once the dust settles 3) **recovery**. In this module, you will deepen your knowledge regarding stages 2 and 3.

Thanks to this module, you will improve your cyber crisis management procedures with steps helping you to deal with the hacker's attack.



Unit 1: Cyber crisis management

Section 1.2: Identify the crisis

First of all, you need to know what may be classified as a cyber crisis.



A cyber crisis is any cyber event that may negatively influence your business.

For example:

- hacked devices
- screen mirroring of your devices
- copied emails
- stolen credit card data
- stolen client database
- crashed websites
- breached networks
- denials of service, etc.






Unit 1: Cyber crisis management

Section 1.2: Identify the crisis

All suspicious cyber events should start your cyber crisis protocol and launch stage 2 – response. Even if you are not 100 percent sure what happened, it is better to initiate an action.

Remember is not only about you and your business's current situation. You have to care also about:

-  your clients and business partners' safety
-  your business' profitability
-  your business' future reputation






Unit 2: Response to the cyber crisis

Section 2.1: The role of time

Your reaction to the cyber crisis has to be fast. Sometimes you have few seconds to do something, and the worse scenario is to start a panic. Keep in your mind that panic and fear may cost you the whole business you build.

The most common cyber crisis mistakes in MSME

-  no designated person(s) responsible for cyber crisis response
-  providers contact info not ready at hand
-  no cyber crisis communication protocol



Unit 2: Response to the cyber crisis

Section 2.1: The role of time

Why do you need a person(s) responsible for cyber crisis response?



Cyber crisis response is any action that may help you manage a crisis event and provide an update to your business' stakeholders.

Cyber crisis response is a plan that you implement in case of an attack. When someone hacks you, there is no time to think who will do what. Everyone needs to be prepared. That's why you need to have one or multiple people responsible for cyber crisis response.

What do you think: the person(s) responsible for cyber crisis response has to have an IT background or not?



Unit 2: Response to the cyber crisis

Section 2.1: The role of time

Are you uncertain of whether the people responsible for cyber crisis response should have an IT background? Well, we can tell you that the IT background is not the most important factor. Why? In the beginning, let's take a look at cyber crisis response person's responsibilities.

Cyber crisis response person's responsibilities

- ✓ to know the backup plan
- ✓ to monitor all activities within crisis
- ✓ to lead the internal strategy
- ✓ to implement the cyber crisis communication protocol



Unit 2: Response to the cyber crisis

Section 2.1: The role of time

If the person responsible for cyber crisis response has an IT background, he/ she may better understand all of the steps involved. However, without the leadership and management skills that are crucial here, an IT person can't implement the cyber crisis response.

If you have a micro-company, it is obvious you need to prepare yourself for that possibility. You can also sign an agreement with a cyber expert that you trust. Small or medium companies should appoint a leader for the cyber crisis response stage.

It is good to remember that the cyber crisis response may be implemented **remotely**.



Unit 2: Response to the cyber crisis

Section 2.2: The backup plan

In MMSE, the backup plan may differ depending on the branch, type of business, etc. However, you should consider the following steps:

Know your providers

Keep all of your providers (Internet, cloud, hosting, etc.) contact information in a secure, unplugged manner. Since the attack can be carried out from your local network, even if you are not connected to the Internet, your passwords and sensitive data may get stolen .

To do:

Consider all possible attacks before they happen. Keep all important contacts not only online, but also in the **printed version**.



Unit 2: Response to the cyber crisis

Section 2.2: The backup plan

Follow the traces

If you notice suspicious actions:

- on your bank account, call your bank and block all credit cards;
- in your business cloud, contact the provider (by phone or e-mail).

To do:

Avoid using apps/ clouds that may be infected. Contact the provider directly.

Pull out the plug!

Sometimes it is the only way to stop the cyber attack.

To do:

If you notice suspicious events on your or your employee's computer/other device, just pull out the plug.



Unit 2: Response to the cyber crisis

Section 2.3: Cyber crisis communication protocol

Thinking about the response to a cyber crisis, you should consider the crisis communication protocol. Here the most important is always time. Communicate as soon as possible with the key stakeholders and inform them about the problem. You should be the source of facts – not the newspapers or social media.

Show your stakeholders you care about them, and you have already taken adequate steps to minimize the cyber crisis consequences.

You have to be ready for this step before the attack, so prepare the key stakeholders list:

- ✓ clients (especially if you have a client database)
- ✓ business partners, sponsors, and investors
- ✓ your suppliers
- ✓ neighbors / other businesses in the building (maybe the attacker hacked them too)



Unit 2: Response to the cyber crisis

Section 2.3: Cyber crisis communication protocol

You also have to consider making a statement on your website/ social media site or in other media. Of course, you can delegate one of your employees to this task.

It is crucial to update your statement frequently. Your stakeholders and audience need to be sure that you take care of their data. Remember that the outcome of the cyberattack may be the future of your business.

How to speak about the cyber crisis?

- ✓ Always speak clearly.
- ✓ Use facts, not opinions.
- ✗ Avoid emotional reactions.
- ✓ Give straight answers to the questions.
- ✗ Do not accuse anyone or apologize until you get to know what happens.



Unit 3: Recovery after the cyber crisis

Section 3.1: How to return to normal after the cyber crisis?

After the cyber crisis, each business needs to take some steps to return to normal functioning. That is how we reach the third stage of cyber crisis management called disaster recovery.



Recovery after the cyber crisis is the process that helps businesses to return to normal operations.

Recovery after the cyber crisis includes post-event steps like:

- ✓ assessments (of the damages, causes, and the management)
- ✓ lessons learned
- ✓ planned improvements



Unit 3: Recovery after the cyber crisis

Section 3.2: Do the assessment!

Recovery starts after the cyber crisis. To make sure that your business will be "healed" you need to take radical steps. First of all, you need to find gaps that may the attack possible.



Plan the assessment meetings with your team to discuss all damages made during the cyber attack. Find and understand the causes. If it is necessary, ask external experts for support.



Evaluate your cyber management plan. Discuss it step by step, all taken actions, to understand what went wrong.



Unit 3: Recovery after the cyber crisis

Section 3.3: Lesson learned

During or after the assessment, create a list of vulnerabilities that made the cyber attack easier. Do not take it personally. Do not think about it as a failure. More important is to learn from this attack.

If you are a leader/ business owner, your attitude has an impact on your employees and stakeholders. If you consider the attack as a failure or wrongly accuse one of your employees of being responsible for it, that may affect your business's future.

Just keep in mind, each move and action you take is influencing not only this moment and this cyber attack but also your future reputation and profitability.



Unit 3: Recovery after the cyber crisis

Section 3.4: Plan the improvements

The last step is to analyze all gaps using facts and data. If you find out that the attacker hacked your business because one of your employees neglected his / her duty, it is better to avoid emotional reactions. There are multiple ways to act in this situation because each case is different.

For sure, you can make an effort to create short- and long-term goals to close gaps. Each gap is a verified indicator in the incident. Each goal assumes the prevention of similar attacks in the future.

The recovery after the cyber attack must eliminate or minimize the causes of said attack. If this does not happen, the lesson won't be learned.



Unit 3: Recovery after the cyber crisis

Section 3.5: Cyber crisis case study

You may be hacked, no matter if you own a small or big enterprise. Owning a bigger company doesn't make you safer or better prepared for the crisis. At least not always. Just take a look at the case studies below.

Marriott International

The cyber attack

The well-known hotels' chain, Marriott International, was hacked in January 2020, but the attack went unnoticed by the company until late February. Hackers who obtained the login credentials of two Marriott employees might gain access to the guest's details. The company started its own investigation.



Unit 3: Recovery after the cyber crisis

Section 3.5: Cyber crisis cases studies

Response

Marriott made a statement that hackers might acquire personal details such as names, birthdates, telephone numbers, language preferences, and loyalty account numbers. Also, the hotel sent emails to the guests involved; created a dedicated website and call center to inform guests. Marriott assured that they carry insurance, including cyber insurance. Till now everything looks professional, however, giving the statement the company didn't believe that its total costs related to this incident would be significant.

Recovery

In October 2020, the UK's data privacy watchdog fined the Marriott Hotels chain £18.4m for a data breach that may have affected up to 339 million guests records.



Unit 3: Recovery after the cyber crisis

Section 3.5: Cyber crisis cases studies

Where was the lesson learned?

First of all, that wasn't the first cyber attack on Marriott International. In 2014, hackers attacked the Starwood Hotels group that was acquired by Marriott two years later. As we know, the company didn't take any recovery steps at that time. That's why the next attack was easier.

The first publicly noticed attack had placed in 2018. Again, the crisis management protocol wasn't implemented correctly, in consequence, until this time the attacker continued to have access to all affected systems, including:

- names
- email addresses
- phone numbers
- passport numbers
- arrival and departure information
- VIP status
- loyalty program numbers



Unit 3: Recovery after the cyber crisis

Section 3.5: Cyber crisis cases studies

That is why Marriott has been fined by the UK's data privacy watchdog. The hotel's chain failed to protect personal data as required by the General Data Protection Regulation (GDPR). Moreover, it failed more than once. Leaders responsible for cyber crisis management didn't identify and analyze gaps deeply.

What helped?

Marriott International carries insurance, including cyber insurance. This helped to pay up the fines.

What can you learn from this?



Unit 3: Recovery after the cyber crisis

Section 3.5: Cyber crisis cases studies

Lessons learned:

- ✓ **Rethink your cyber crisis management.**
- ✓ **Think if you have enough leadership and management skills to implement the cyber crisis management plan.**
- ✓ **If not, learn more in our other courses.**
- ✓ **Also, look for a cyber expert as support.**
- ✓ **Think whether you need cyber insurance.**



Unit 3: Recovery after the cyber crisis

Section 3.6: Summary

Nowadays, cyber crisis management is important the same for a micro and large company.

The difference is in the resources that you have. The smallest business the biggest responsibilities you have as an owner.

Remember that a cyber crisis may affect your company even if it is not a typical online business (e-business). Whenever you need a laptop, smartphone, printer, fax, mailbox, you need to consider cyber security management.

Finally, keep in mind that mismanagement may escalate the crisis or even create a new one.

Good luck!



Bibliography and relevant links

The New Statesman > **How to tell your customers you've been hacked**

<https://www.newstatesman.com/spotlight/2019/09/how-tell-your-customers-you-ve-been-hacked>

Deloitte > **Cyber crisis management: Readiness, response, and recovery**

<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf>

Security Boulevard > **Marriott Data Breach 2020: 5.2 Million Guest Records Were Stolen**

<https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/#:~:text=The%2520breach%2520was%2520identified%2520at,have%2520accessed%2520the%2520guest%2520details>

BBC News > **Marriott Hotels fined £18.4m for data breach that hit millions**

<https://www.bbc.com/news/technology-54748843>

Marriott International News Center > **Marriott International Notifies Guests of Property System**

Incident

<https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident>

Forbes > **What Businesses Are The Most Vulnerable To Cyberattacks?**

<https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=1c1c8f663534>



Thank you for your attention!

