advenica

CISO

Your guide to cybersecurity

How to work successfully with cybersecurity as CISO

CISOs face many challenges when working with cybersecurity. There are not only laws you must follow, but also best-practices that can help you avoid pitfalls and security risks along the way. And even if you have a clear plan of how you should work with cybersecurity, it can be difficult to explain to the management team that cybersecurity needs resources in order to protect your business. In this guide, we present three articles that can teach you about important laws to be aware of, security risks you should avoid, and how you convince management to prioritise cybersecurity.

Articles

- CISO – How you make sure that the management team prioritises cybersecurity
- A stricter Protective Security Act: 3 things the CISO needs to consider
- The security risks the CISO must be aware of

CISO – How you make sure that the management team prioritises cybersecurity

Digitalisation has led to cybersecurity becoming increasingly important, but it does not always receive the priority it deserves. It is not always easy for the CISO to explain to the management team why working with cybersecurity is so important. Here are some things to keep in mind during a presentation for the management team.

With more and more devices connected to the Internet, possible attack routes into the IT infrastructure are increasing. All companies and authorities need to ensure that they do what they can to avoid an attack. A structured approach to cybersecurity is therefore something that must be in place. But how do you go about securing the management team's commitment?

1. Analyse the risks

In order for you to be able to make the right priorities in your security work, some sort of risk analysis is needed – a security protection analysis. It determines the protection values of the business, the consequences that can arise if these protection values are attacked, what the threat is and what vulnerabilities there are. Based on this, appropriate protective measures can then be proposed. By asking yourself a number of questions, you can deliver a security protection analysis that allows you to be very concrete when you present to the management team or the IT manager.

You might have to meet the requirements of the Protective Security Act. The Protective Security Act[1] (2018: 585) contains requirements for measures aimed at protecting information that is important for Sweden's security, or that is to be protected in accordance with an international commitment on security protection. The law also applies to the protection of other security-sensitive activities, such as information systems important for society. If you are covered by this law, you have a clear argument for why you must prioritise your cybersecurity.

1 'What does the new security law mean' from https://advenica.com/en/what-does-the-new-security-law-mean

2. Explain the consequenses

You must reveal what the consequences could be if you neglect cybersecurity. There are several known cases of ransomware attacks, such as the Maersk case[2]. You can also include more relevant examples based on your analysis. For example, if you have discovered that you have shortcomings in your software updates, it is more communicative and convincing to say that "a hacker can copy the entire payroll and post it on the internet" than to talk about the need for several security updates. So, adapt the scenario of consequences to your business and what you need to protect.

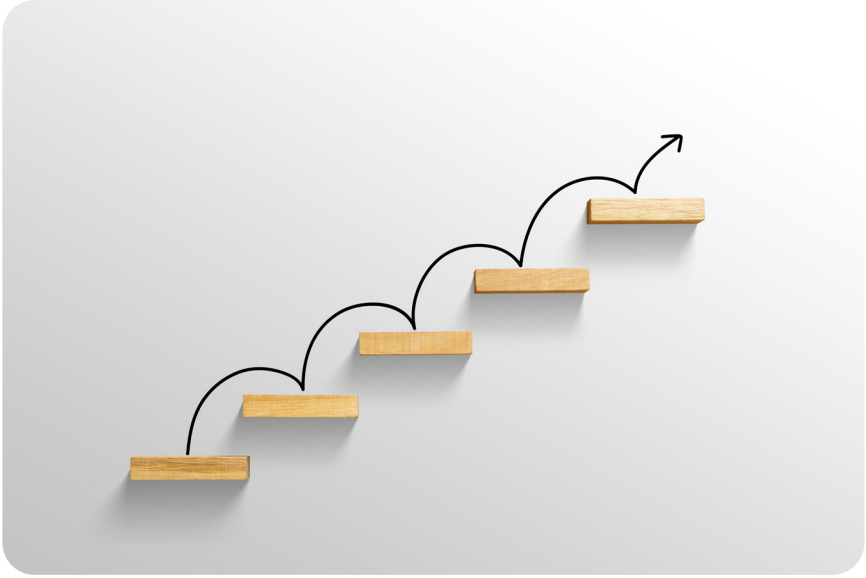
2 'Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks' from https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

3. Show how you can save money

A counterargument you can get is: "But does it not cost a lot to introduce a structured approach with information security?". This is something you can quickly respond to by explaining that the cost of an attack is usually much higher than the investment needed for higher security. With an ever-increasing number of attacks, the risk of being affected is relatively high. Not investing in your cybersecurity therefore actually mean that you take an extremely large financial risk. Ask the management team if they really want to take that risk?

4. Elevate the benefits

It is good if management associates cybersecurity with something positive and uncomplicated. Therefore, it is important that you end the presentation with explaining that systematic cybersecurity work allows you to avoid negative publicity, information leakage, downtime – you can simply avoid several risks that could lead to lost business. Another positive effect of structured cybersecurity work is that employees have access to the right information at the right time, which often increases efficiency. By emphasising these, and other benefits of structured cybersecurity work, it becomes easier to secure the management's commitment.



A stricter Protective Security Act: 3 things the CISO needs to consider

The new, stricter Protective Security Act will enter into force on December 1st 2021, if the government's proposal passes. Before that, the CISO needs to be aware of what applies – here are the most important things.

What is the Protective Security Act?

The Protective Security Act (2018:585) clarifies the obligations of those who conduct security-sensitive activities and the importance of operators conducting security protection analyses for their activities. Security protection means preventative measures to protect Sweden's security against espionage, sabotage, terrorist crimes and other crimes. The technological development in recent years means that we need to broaden the concept of security. In addition, public sector organisations and private companies should now also be included within the frame of security protection.

The law will apply to activities in both public and private sector, and those concerned can seek support and advice from the Security Service and the Armed Forces, or other supervisory authorities. A new aspect is that businesses with data worth protecting are covered, without being officially classified as secret. This can, for example, be about critical infrastructure and their systems for operation, since these represent a potential vulnerability. The government is now proposing that the present Protective Security Act will become more strict. The amendments to the law are proposed to enter into force on December 1st, 2021.

1. Security protection agreements apply to more types of collaborations

Part of the new proposal is that the security protection agreement included in procurements will now apply to all types of collaborations where the other party can gain insight into security-sensitive activities. These agreements may also need

to be established with subcontractors to the actor with whom you are about to enter into cooperation with. The agreement must be entered if the actor, through the cooperation, can gain access to security-classified information classified as confidential or higher, as well as information about the business that can be considered to have an equal degree of significance for Sweden's security.

2. Certain security protection assessments must be carried out

Outsourcing and similar situations that require security protection agreements must undergo special security protection assessments. This is to be able to determine whether the procedure is appropriate or not from a security protection point of view. The assessment shall, among other things, review which security protection classified information that the collaboration partner can access, as well as which information about security-sensitive activities they can handle. If it turns out that the collaboration is not inappropriate, the supervisory authority must be consulted before the collaboration begins.

3. Supervisory authorities get a larger role

Another aspect is that the supervisory authorities will be given more power to investigate security protection and any shortcomings. If it becomes apparent during an inspection that the requirements have not been met, the shortcomings that the supervisory authority has discovered must be handled immediately.
The supervisory authority shall also have the right to issue fines and sanctions if an operator has not complied with the obligations that apply. This may apply, for example, if you have not controlled your security protection or if you have not controlled that a partner complies with the security protection agreement. If you do not follow the regulations, you can receive a penalty fee of up to 50 million SEK.

Read the whole proposal for the Protective Security Act[3] (in Swedish)!

3 'Ett starkare skydd för Sveriges säkerhet' from https://www.regeringen.se/rattsliga-dokument/lagradsremiss/2021/03/ett-starkare-skydd-for-sveriges-sakerhet/

The security risks the CISO needs to be aware of

Today's modern technology makes us vulnerable and security risks are constantly increasing. A CISO needs to be aware of a lot to avoid the vulnerabilities if being exploited to a cyberattack – something that can have enormous consequences both for the company and for society. We describe six important security risks that you should be aware of.

Technology dependence creates security risks

The world is more dependent on technology than ever before. Companies and authorities store a lot of data on computers and send it over open networks to other computers. Many systems are interconnected and as digitalisation continues, more and more systems will be interconnected.

Digitalisation is not only positive – it also means that we become more vulnerable. Different entities and their underlying systems have vulnerabilities that can undermine the well-being and goals of an organisation. And the problem is that vulnerabilities are used for cyberattacks.

What can a lack of information security lead to?

Lack of information security can have consequences such as business not being able to be conducted in an appropriate and efficient manner, lack of protection of personal integrity and disruptions in socially important activities.

Deficiencies in information systems can also affect physical assets. Damage to critical infrastructure can have fatal consequences. Incidents that lead to the inability or destruction of such systems and assets can lead to serious crises affecting the financial systems, public health, national security, or combinations thereof. It can also lead to a deterioration in confidence in services and underlying actors. Serious and repeated disruptions can lead to crises of confidence, which can also spread to more actors and services, as well as to other sectors.

Risks you should be aware of

1. Remote control of systems

Many organisations depend on remote access via RDP, for example for suppliers to be able to perform maintenance, or for operating personnel to be able to monitor a facility. Sometimes, general connections such as IPsec or TLS are used to connect computer networks remotely. In terms of IT security, such connections mean that both systems are exposed to the sum of the threats that apply to one of the two systems. This also means that there are risks of both incorrect configuration and implementation bugs. Secure remote access solves many of the security risks that are otherwise associated with such solutions.

2. Integration of IT/OT systems

Operational Technology (OT) is a term that includes all the subsystems needed to control and monitor a physical process, such as a power plant or a factory. IT refers to the business and office-based systems that most organisations use. Digitalisation means that IT and OT systems need to be connected, and often the same type of technology is used in IT and OT. The different needs in IT and OT easily lead to technical conflicts that can be challenging to handle. With secure solutions, you can maintain accessibility and at the same time increase security.

3. Traceability and logging in security-sensitive operations

Most IT systems generate logs that enable troubleshooting and traceability. To benefit the most from such logs, it is important to combine logs from as many systems as possible in one chronological list.

If you have security-sensitive or zoned systems and want to implement centralised logging, you need to resolve an inherent goal conflict. Logging benefits from having one shared system for all zones/subsystems, but a shared system also increases the risk of attacks. To reduce the risks, a solution is required that protects both log information and all connected systems.

4. Transmission of SCADA information

For many years, companies using SCADA systems have been gradually automated. At the same time, the systems have become increasingly complex and control more and more socially critical functions. This makes them more vulnerable and the challenge will be to continue digitalising in a secure way. At the same time, the need to transfer the information to other networks to be able to work efficiently is growing.

However, transferring socially critical information, for example from a SCADA system to an administrative office network, involves potential security risks. Here, secure solutions are needed that take care of security issues and at the same time enable an exchange of information.

5. Updates

Since starting with Windows and/or Linux-based systems, the need to be able to update these systems has increased. This need is due to the fact that complex software often contains bugs that should be fixed to ensure stability in the systems. But making these updates is something that in itself can pose a security risk if not

done properly. The integrity and availability of the systems must be maintained and most system updates are normally not sufficiently evaluated in the environment in which they are used, or in combination with the applications running. To avoid the risks and to maintain the integrity and availability of the systems and be able to make secure updates, special solutions are required.

6. The security culture

Cybersecurity today is not only a technical challenge but also a human challenge – it is a matter of security culture. Criminals do not always use only technical shortcomings, but often rely on people to access sensitive data. Therefore, the human factor is the main cause of the most serious security breaches. Building and maintaining a strong security culture is thus an extremely important part of working with cybersecurity.

To become better at security culture, attitudes and behaviors need to change. The organisation needs to see cybersecurity and security culture as a critical activity for the whole company and not as an isolated IT issue – it is also important that the management prioritises the issue. What should define the work with security culture is to think of security as something that enables the work, not as an obstacle.

In our customer cases, you can read more about the challenges our customers have had and how solutions from Advenica raised the level of cybersecurity, increased preparedness for threats and gave the customer increased security insight.

If you want to know more about how security solutions can secure your information and protect your business from cyberattacks, you are welcome to contact us!

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

advenica

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED