ETHOS Cyber Security Incident Response Planning

ETHOS

ETHOS Cyber Security Incident Response Planning

Cyber Security has become an increasing imperative for health and care businesses and services. ETHOS response planning aims to facilitate improvements across the sector, building on what works and ensuring it is fit for purpose.

Cyber-attacks take many forms, ranging from simple phishing scams, virus infections of networks and systems, social engineering of staff or vulnerability scanning of the network, looking for pivot points through to persistent dedicated attacks aimed at penetrating your security to disrupt business operations or steal intellectual property.

The focus of the incident planning needs to address these questions:

- If the worst should happen, how prepared are we?
- Do we have a fit for purpose Cyber Security Incident Response Plan?
- Could we respond quickly and decisively to enact a kill-chain to end the attack?
- How quickly could we recover our business-critical services?
- How would we prevent a repeat attack attempt?
- What is our worst-case scenario?

ETHOS can help you define and implement your Cyber Security Incident Response Plan and train your employees, so they understand what role they play in the Response Team (CSIRT). We can also be on standby to either lead your CSIRT or provide essential resources in the moment you need them most.

Cyber Security Incident Response Plan (CSIRP):

The CSIRP should use a structured methodology, defining how it will handle cyber security incidents, breaches, and threats. A well-defined plan allows you to effectively identify, minimize the damage, and reduce the cost of a cyber-attack, while finding and fixing the specific attack vector to prevent similar attacks in the future.

Best practice suggests your CSIRP should be comprised of 6 stages:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

ETHOS

Cyber Security Incident Response Team (CSIRT):

Part of the planning activity will need to address the issues of resourcing your Cyber Security Incident Response Team; those individuals responsible for enacting the CSITP. There are three primary models to consider:

- Employees: the organisation conducts all incident response-related activities by itself, without any guidance or intervention from external parties.
- Partially Outsourced: the organization outsources certain elements of its incident response-related activities to external parties.
- Fully outsourced: the organization outsources all elements of its incident response-related activities to external parties.

A brief guide to ETHOS methodology for CSIRP

Stage 1: Preparation

This phase will be the most crucial phase to protect your business and includes:

- Well trained staff, confident in their incident response roles and responsibilities in the event of an attack.
- Developed incident response test scenarios, regularly conducting simulated data breaches to evaluate the incident response plan.
- Approved incident response plan (training, execution, resources, etc.), approved in advance.
- Well documented, clear roles and responsibilities.
- Tested to assure performance of staff and any third-party resources, reducing the likelihood they will make critical mistakes.

Questions to address therefore are:

- Has everyone been trained on security policies?
- Have security policies and the incident response plan been approved by appropriate senior management?
- Are Cyber Security Incident Response Team confident and competent in their roles and responsibilities?
- Have the Incident Response Team members participated in simulated attacks that were honed for your objectives?

Stage 2: Identification

This process determines whether you have been breached or if your systems have simply identified a false positive. A breach, or incident, could originate from many different areas.

Questions to address:

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it directly affect operations?
- Has the source and/or pivot point of the breach been discovered?

Stage 3: Containment

Once discovered, the initial instinct may be to securely delete everything so you can just get rid of it. However, that will destroy valuable evidence that you will need to determine where the breach started and devise a plan to prevent it from reoccurring.

Immediate steps to take:

Contain the breach so it does not spread causing further damage to your business. If you can, disconnect affected devices. Have short-term and long-term containment strategies ready. Use a system backup to restore business operations. That way, any compromised data is not lost forever. This is also a good time to update and patch your systems, review your remote access protocols (requiring mandatory multi-factor authentication), change all user and administrative access credentials and harden all passwords.

Questions to address:

- What has been done to contain the breach short term and longer term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all access credentials been reviewed for legitimacy, hardened, and changed?
- Have you applied all recent security patches and updates?

Stage 4: Eradication

Once contained, you need to find and eliminate the root cause of the breach and better understand the attack vector.

Immediate steps to take:

All malware should be securely removed, systems should again be hardened and patched, and updates should be applied. Whether you do this yourself or hire a third party such as ETHOS to do, a thorough approach is essential. If any trace of malware or security issues remain in your systems you may still be losing valuable data, and your losses could increase.

Questions to address:

- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened, patched, and updates applied?
- Can the system be re-imaged?

Stage 5: Recovery

The process of restoring and returning affected systems and devices back into your business operations, focuses on getting them up and running again without the fear of another breach.

Questions to address:

- When can systems be returned to production?
- Have systems been patched, hardened, and tested?
- Can the system be restored from a trusted back-up?
- How long will the affected systems be monitored and what indicators will require monitoring?
- What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)

Stage 6: Lessons Learned

On completion of the above process, hold a lesson learned meeting with all CSIRT members and discuss what has been learned from the data breach - analyse and document everything. Determine what worked well in the response plan, and where improvements could be made. Lessons learned from both simulated and real events will help strengthen the controls to protect systems against future attacks.

Questions to address:

- What changes need to be made to the security?
- How should employee be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach does not happen again?

Whatever the model, then ETHOS is here to help augment your team with specialist resources, available when you need them most. This business-critical element of working in the sector is in safe hands with ETHOS team. For advice and a bespoke package of support please contact us.

For more information about ETHOS safety and innovation work please find us on:

@LtdETHOS

linkedin.com/company/ethos-ltd

or email us at: info@ethos.co.im