Incident Readiness

How to prepare for a cyber incident

CHECKLIST

Cyber attacks and data breaches are inevitable. It's important to prepare your organisation and know how to respond quickly and appropriately. In this checklist, we take you through the key components of an 'incident readiness plan' to help you limit the damage of a hack.

Capabilities — Know your own technical capabilities in detail. Make a record of your strengths and weaknesses, the security measures you have in place as well as the gaps you haven't covered.

Forensic Readiness — Make sure you are prepared for any forensic investigation. Consider the size of your network and associated traffic, the number of systems you have, which sources and logs are available and what information can be collected. If possible, turn on logging for at least 30 days.

Help Lines — Know the existing help lines and make sure they are available in the event of a cyber incident. When in doubt, always contact Eye Security's Incident Response Team to assess the situation quickly and correctly.

Crisis Organisation — Make internal agreements in advance about the circumstances that merit an escalation to the crisis team. Determine what the crisis team will look like and decide which roles will be filled by whom. Agree on the reachability and availability of the crisis team.

Legal — Map out which authorities need to be informed in case of a hack or data breach and identify options for specialised legal assistance in case of an incident.

Communication — Consider how you will communicate if the company network is down. Keep in mind that standard means of contacting employees, customers and suppliers may not work. Don't use a potentially hacked system for communication as the attacker could see the information.

Business Continuity — Develop alternatives to ensure business continuity. Determine which systems in your network are most critical. An incident response party can account for these systems at the time of an incident.

Back-ups — Develop a backup strategy with immutable backups and regularly check their health and security. Conduct periodic tests on restoring backups.

Insurance — Take stock of the financial consequences of a cyber-attack on your organisation. Investigate whether you are insured against a cyber attack and to what extent you meet the policy conditions. Agree and know who is contacting the cyber insurer in case of an incident.

Evaluation — Define when the crisis will end, how you will come to that decision and how you will communicate it. It is important that the business does not suffer unnecessarily because you remain in 'crisis mode' for too long.

If you get hit by a cyber-attack or data breach, don't hesitate to contact us. Eye Security's Incident Response Team is available 24/7 to get your business operations back up and running. Give us a call on +31 886444898 (available 24/7).

www.eye.security info@eye.security