Loss Prevention Standards – Asset Classes

Cyber Security - Respond and Recover

Version: 1.2
Date: 06th August 2024

Cybercrime can be a major problem for businesses. How an organisation responds to any incident, will determine how quickly and how fully it can recover.

AVIVA

Cyber Security: Respond & Recover

Introduction

Cybercrime has increased dramatically, with criminals taking advantage of the proliferation of devices, familiarity and compliancy by users, and an increase in homeworking to get access to individuals and companies' systems and procedures.

Knowing how to respond to any cybercrime incident in a speedy and comprehensive manner could:

- ✓ Minimise the impact of the incident, both in the short and long term.
- ✓ Protect the reputation of the business, and its market position.
- ✓ Support IT security enhancements, by learning from incidents.
- ✓ Minimise or prevent reoccurrences.

The Process

When looking at responding to a cyber incident and recovering systems to a previously secured position, cyber professionals and the National Cyber Security Centre recommend a 5-step approach:

1. Prepare
2. Identify
3. Restore
4. Report
5. Learn

Step 1 - Prepare

The first step is essential, as being prepared for what might happen will help reduce the chances of attack, as much as possible, and minimise any impact, should an attack occur.

Using a Likelihood vs Severity table, like that shown below, will help an organisation focus on the correct incidents.

Very Likely					
Likely					
Moderate					
Not Likely					
Rare					
	No Impact	Little Impact	Moderate	Some Impact	Catastophic

Plotting possible incidents, should show the priorities for attention at this stage

Management buy-in at the senior level of a business is critical. Part of the preparation would be to include 'what to do to protect what is at risk', as an agenda item at management meetings and to discuss it regularly.

Understanding what the critical information is, where it is stored and what systems, software, processes etc., used by the business and how these are accessed, is key to understanding what is needed to be done at this stage.

✓ Password management and user privileges are other actions that an organisation needs to manage effectively.

Key and essential data should be backed-up at least daily. Duplicate back-ups, if possible, should be undertaken with at least one copy being stored off-site. "Mirroring" of data between two locations would see two live copies of data at all times.

✓ Testing the back-ups, and a full restore from back-up will alert an organisation to any weakness in these arrangements.

Employee training should be high priority, with trained individuals being aware of what cyber crimes are, and what they can look like.

✓ Phishing attacks can be convincing but can also have tell-tale signs that there is something not quite right about the text, email, etc.

Who else is a business connected with? It could be that as part of the preparation process, discussions with business partners, suppliers, and key customers should occur, detailing what actions need to be taken in the event of a cyber incident.

✓ Having a dedicated contact would speed up any actions needing to be taken.

Contacts such as these, and details of any person or company needed to assist in the event of an incident, should be formally documented in an Incident Plan. Employees will need to be allocated certain responsibilities in the event of an incident and for some roles 'deputies' should be considered for periods of absence.

✓ Once in place the Incident Plan should be kept securely in both hard copy and electronic formats…and in several locations with at least one copy off-site.

The Incident Plan should be reviewed regularly to check for its accuracy and tested to ensure it works as desired. Both should be completed at least annually and/or associated with any changes.

✓ Where required it should be updated as necessary.

Step 2 - Identify

Step two is to identify what has happened or is happening. There are some signs that may show that systems may have been infiltrated such as:

- Computers running slower than normal
- Redirected internet searches
- Documents becoming locked
- Unusual email correspondence
- Unauthorised payments
- Ransom being demanded

The National Cyber Security Centre recommends ten questions to help assess and identify what might have occurred:

1. What problem has been reported and by who?
2. What isn't working?
    - Hardware?
    - Software?
3. Has data been lost?
4. What data has been accessed, deleted, or corrupted?
5. Have there been any reports from customers?
    - Do they still have access to systems, orderings, etc?
6. When was the problem first noticed?
7. Does the problem affect systems or departments, or is it company-wide?
8. Who designed the affected system?
    - Who maintains it?
9. Are there any impacts on your supply chain?
    - Did the issue originate somewhere in the supply chain?
10. What is the potential business impact?

The next step is to review your 'anti-virus audit logs' for a cause and complete a further full scan.

Step 3 – Restore

This stage is for:

✓ Resolution of the incident
✓ Getting back to business
✓ To replace the affected hardware and software
✓ Ensuring all security is in place
    - Part of reviewing security is to ensure all updates and patching has been done and passwords have been changed, etc.
✓ Restoring data from back-ups.

Step 4 - Report

In the UK, it is essential that attacks are reported fully and swiftly to Action Fraud.

- This is the UK's national reporting centre for fraud and cybercrime or agencies responsible for cybercrime in your country or local area.
- In other territories please establish the local equivalent.

Promptly reporting of attacks helps to spread the details of the type of attack, so other organisations can be more prepared. It also gives the Police additional information to help the apprehend the criminals.

Also, report the information internally to employees, as this will show individuals what to look out for and encourage them to be more vigilant. It can also alert people to the fact that their own personal details might have been compromised, if say online purchases or banking had been undertaken on work equipment.

✓ Passwords, etc may also need changing.

Step 5 – Learning

Post incident, a formal review of what happened, what was affected, what was lost, any effect on customers or the supply chain, and any other information is very important. There will be learnings in the activity taken as part of the response process, such as what worked well and what needs to be improved. There are likely to be lessons learnt from a prevention point of view, and employee training can be one of them.

- ✓ It may be that phishing exercises or awareness sessions should be held.

Physical and electronic security will need to be reviewed. This could result in upgrades being required to prevent a repeat incident, be it more rigorous access controls or removing access to say a machine's USB ports etc.

A formal review of the following will be required and revised as appropriate, based on any learnings:

- ✓ Likelihood vs Severity matrix
- ✓ Incident Plan

This will help ensure an organisation is still concentrating and focussing on the correct issues.

A Final Thought…

Time is very much of the essence when responding to a cyber-attack. This includes contacting and getting appropriate trained security professionals into the organisation as early as possible… ideally within the first 72-hours. This time element factor is key to an effective recovery.

Also, if you have Cyber insurance, inform your Insurer and Broker as soon as possible, to allow them to support any response needed.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solution-Specialist Partners

Sources and Useful Links

- National Cyber Security Centre (NCSC)
- ActionFraud

Additional Information

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666. *

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

06th August 2024

Version 1.2

ARMSGI252024

LOSS PREVENTION STANDARDS