Loss prevention standards

# Cyber Security:

# Respond and Recover

Cyber crime can be a major problem for businesses. How your organisation responds to any incident, will determine how quickly, and how fully you can recover.

AVIVA

# Cyber Security: Respond and Recover

## Introduction

Cyber crime has increased dramatically during the Coronavirus pandemic, with criminals making every effort to take advantage of companies and individuals, when they and their systems and procedures are at their weakest, stretched by remote working and other issues caused by normal places of work being unavailable.

Knowing how to respond to an infiltration, in a speedy and comprehensive way, could:

- Protect your ability to provide what you do for your customers
- Help update and improve your security, from incident learnings
- Minimise the impact of the incident, both in the short and longer-term
- Protect your reputation as a business, and your market position

## The Process

When looking at responding to a cyber incident, and recovering to a position where you are secure, and providing for your customers, cyber professionals, and the National Cyber Security Centre, recommend a 5-step approach:

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

### Step 1 - Prepare

This first step is essential as being prepared for what might happen will help minimise the chance of attack as much as is possible, and also minimise the impact should an attack happen.

Using a Likelihood vs Severity table, similar to 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.

Buy-in at the senior level of a business is also key, and part of the preparation would be to include what you do to protect what's at risk, as an agenda item in team and management meetings.

Understanding what is the critical information, where it's stored, and what systems, software, processes your business uses, and how these are accessed is also key to understanding what may need to be done at this stage. Password management and user priviliges are among other actions that organisations should effectively manage.

Data back-ups of key data, at least daily, are essential. 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 you to any weaknesses in the arrangements.

Staff training should be a high priority, with staff trained to be 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's something not quite right about the text, email, etc.

Who else are you connected with? It could be that as part of the preparation process, you should discuss with business partners, suppliers, and key customers what actions would 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 you would need to assist you in the event of an incident, should be put into an Incident Plan. Members of staff will need to be allocated responsibilities in event of an incident needing action, and deputies considered for periods of absence. Once in place the Incident Plan should be kept in hard copy format and electronically, and at more than one location, with at least one copy off-site.

The Incident Plan should be regularly checked for accuracy, tested to ensure it works, and updated where necessary.

### Step 2 - Identify

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

- Computers running slow
- Redirected internet searches
- Unauthorised payments
- Documents becoming locked
- Ransom being demanded

The National Cyber Security Centre recommend ten questions to help assess and identify what has occurred:

- What problem has been reported and by who?
- What isnt working? Hardware? Software?
- Has data been lost?
- What data has been accessed, deleted or corrupted?
- Have there been any reports from customers? Can they still access systems, ordering, etc?
- When was the problem first noticed?
- Does the problem affect particular systems or departments, or is it company-wide?
- Who designed the affected system? Who maintains it?
- Are there any impacts on your supply chain? Did the issue originate somewhere in the supply chain?
- What is the potential business impact?

The next step at this stage is to review your Anti-virus audit logs for a cause, and complete a further full scan.

### Step 3 - Resolve

This stage is resolution of the incident, and getting back to business, to replace affected hardware and software, ensuring all security is in place, and restoring data from back-ups.

Part of reviewing security is to ensure all updates and patching has been done, and passwords are changed, etc.

### Step 4 - Report

It is essential that attacks are reported fully and quickly to Action Fraud, which is the UK's national reporting centre for fraud and cyber crime. The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB).

Promptly reporting attacks helps to spread the details of the type of attack so others can be prepared, and gives Police information with which they can attempt to apprehend the criminals.

Also report the information internally to staff, as this will show individuals what to look out for, and encourage them to be 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 need to be changed.

### Step 5 - Learn

Post incident, reviewing what happened, what was affected, what was lost, affect on customers, and any other key information, is very important.

There will be learnings in activity taken as part of the response process, such as what went well and what needs to be improved?

There are likely to be learnings from a prevention point of view also, and staff training could be one. It may be that a phishing exercise, or an awareness session should take place.

Physical and electronic security will need to be reviewed, which could result in upgrades required to prevent a repeat incident, whether that's access controls, or removing access to USB ports, etc.

Updating of the Incident Plan in event of any learnings, and a re-assessment of the Likelihood vs Severity matrix, will help to ensure that following any changes you are still concentrating on the correct issues.

## A Final Thought…

Time is very much of the essence when responding to a cyber attack, and this includes contacting and getting-in security professionals as early as possible as the first 72-hours are key.

Also, if you have Cyber insurance, informing your Insurers as soon as possible will allow them to aid your response.

## Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

## Sources and Useful Links

- The National Cyber Security Centre
- Action Fraud

## Additional Information

Relevant Loss Prevention Standards include:

- Pandemic Planning & Coronavirus
- Pandemic Recovery: 'New Normal' and the Post-Pandemic Business World
- Cyber Security: Top 12 Tips to Protect Against a Cyber Attack
- Cyber Security: Social Engineering
- Cyber Security: Cyber Essential Accreditation

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.*

*Calls may be recorded and/or monitored for our joint protection.

## 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.

04/09/20 V1.0

Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

LOSS PREVENTION STANDARDS