InfoTrust

EXECUTIVE SUMMARY

# RESPONDING TO CYBER ATTACKS

With the recent global digital pandemic of cyberattacks, it is now established that cybercriminals have become a sophisticated class of criminals with a full array of digital tools at their disposal. This phenomenon, coupled with other disturbing statistics around increasing phishing and social engineering attacks, should be treated with the utmost importance. In fact, 74% of IT decision-makers say targeted phishing attacks are their biggest concern.

74% Of decision makers are concerned about phishing attempts making their way to end users

These cyberattacks, from the organisation's perspective, are information security incidents capable of compromising business operations and threatening data security. This article provides an overview of how to prepare an organisation for dealing with a cyber-attack as well as strategies to ensure appropriate steps are carried out while minimising the impact.

## WHY HAVING AN APPROPRIATE RESPONSE PLAN MATTERS

In business, regardless of the security measures in place, incidents happen. The severity of the damage is directly correlated to the nature of the incident but also, and more importantly, to how it's handled. When a security incident occurs, it's vital that it is dealt with promptly and appropriately. When the correct response plan is in place, individual risk, operational damage and financial, legal and reputational costs are drastically reduced.

## HOW TO DEFINE A SECURITY MANAGEMENT RESPONSE PLAN

To define a security management response plan, organisations need to specify the scope, stakeholders and expectations in the event of a security incident. The following steps enable the appropriate information to be gathered to start to define how security incidents will be handled:

1. **Scope** - In today's cloud-connected world, incidents around an organisation's information and data can take place outside of its networks and systems. Organisations should consider defining the scope based on its key assets, including not only networks and devices but also data and services.

2. **Stakeholders** - Organisations should define who could be affected by an information security incident. This should include anyone who could become aware of the incident, at the very least employees, contractors, customers, suppliers and other third-parties should be considered.

3. **Processes and procedures** - These need to be developed to cover the training of employees and contractors to notice and report a potential incident, the reporting of incidents promptly through appropriate channels, and responding to and documenting incidents as they happen. There should also be a process around knowledge gathering and data collection and using this to reduce the likelihood of future incidents.

4. **Expectations** - Research should be carried out around the reporting, management and response to information security incidents based on their potential to cause harm.

## THE IMPORTANCE OF CLEARLY DEFINED ROLES AND RESPONSIBILITIES

When an information security incident has been declared, an organisation's employees quite often react in different ways. Everyone aims to try and resolve the issue as soon as possible or in the best way, but this ad-hoc approach can lead to more issues. Therefore, it is important that organisations define a clear process, as well as clear responsibilities for everyone that would be involved in an information security incident.

As security incidents often require communication with both internal and external stakeholders, the appropriate action needs to be considered to avoid unnecessary communication. Organisations should ask themselves who needs to know about an incident, when they need to know and the critical points that should be communicated and why.

# **KEY STEPS** IN RESPONDING TO AN INFORMATION SECURITY INCIDENT

There are four key steps to responding to an information security incident:

1. **Conduct an Initial Impact Assessment** - The first step in responding to a cyber incident is to calculate the extent of the damage and the impact it has on the organisation's operations. This will allow organisations to determine the severity of the incident and prioritise the plan of action. Information security incidents can range from devices that are damaged but have their files backed up to the theft of a customer database. The most significant consideration of any assessment is the potential for adverse consequences to individuals. Organisations should consider how serious the risk is to individuals alongside the likelihood of the risk occurring.

2. **Take Appropriate Steps to Minimise Further Damage** - Once the impact assessment has been completed, an organisation should create a plan of action on how to minimise further damage to its operations. Information security incidents need to consider the initial response which investigates and contains the situation and also a recovery plan to reduce the extent of any damage. This will often involve input from specialists across the business such as technical management, legal response and in some cases, contact with external stakeholders and suppliers.

   All information security incident treatment should include the following activities:

   - **Containing the incident** - this may include unplugging affected computers from the network, changing passwords, etc.
   - **Removing the cause** - determining and removing the cause of the incident and performing additional vulnerability analysis.
   - **Communicating with internal and external parties** - to include disclosure of potential breaches to affected individuals, where required by law.
   - **Reassigning action** - removing areas of work outside of the incident management process to maximise business operations.
   - **Restoring and recovering affected systems** - aiming to get systems back up and running so business-as-usual can be restored as quickly and effectively as possible.
   - **Updating the incident management database** - including logging information, discussing the incident and communicating lessons learned.

3. **Develop a Comprehensive Communications Plan** - To build a communications plan, firstly, organisations should identify all stakeholders involved, both internal and external. For each stakeholder, a clear and precise communication message should be drafted and approved. This ensures that there are no overlaps and that each stakeholder's individual needs are catered to. It should be assumed that everything published internally will at some point become an external communication. Therefore, it is imperative that any internal communications should not be contradictory to those developed for external stakeholders.

   The next step should be establishing a communications schedule and the channels that will be used (email, website, etc.). Communications should be supported by a list of frequently asked questions (FAQ) for staff to refer to. If there are any unknowns, organisations should indicate as such rather than adding erroneous information.

   When dealing with external communication, the following "TO CRACK" principles will assist in preparing a consistent, comprehensive and unified approach:

   - **Timeliness** - do not delay communications once an incident has occurred.
   - **Ownership** - ensure that there is a single, accountable C-level owner.
   - **Clarity** - use simple and clear language.
   - **Restraint** - provide only as much information as required.
   - **Accuracy** - present information in a factual manner.
   - **Compassion** - display sincerity in communications.
   - **Knowledge** - make a list of all information and any lacking information.

4. **Notify and Respond to Stakeholders** - Organisations should aim to disclose information as soon as realistically possible. This shouldn't be rushed, however. Organisations should have a degree of certainty about the incident and have a clear reason as to why they are disclosing information.

When it comes to incident communication, there is no silver bullet or one-size-fits-all approach. Each incident will have a unique situation and involve different types of stakeholders. Therefore, each incident will require a separate kind of communications plan. Communication options include:

- Websites - dedicated sites to answer possible questions and serve as a focal point.
- Social media - allows for quick updates, but the narrative can get diluted and isn't easily controlled.
- Email - directly contacts stakeholders but is an easy approach and doesn't show as much empathy as other channels.
- Press release - communications can come across as too polished or manufactured.

The choice in communication will depend on the size of the organisations and the scale of the incident. However, the most important aspect is to communicate what has happened in an honest and straightforward manner.

Organisations should proactively develop a paradigm or framework that allows them to deal with information security incidents in a consistent, effective and diligent manner. With every incident, the organisation should consider affected stakeholders and draw up a communication plan that factors in their dynamics, as well as relevant messaging timelines.

Perhaps the most essential aspect of incident management is practising restraint in order to minimise any unintended information disclosure that could further compound the issue. And, creating a database of incidents allows organisations to learn and reduce future risk.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, InfoTrust, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.