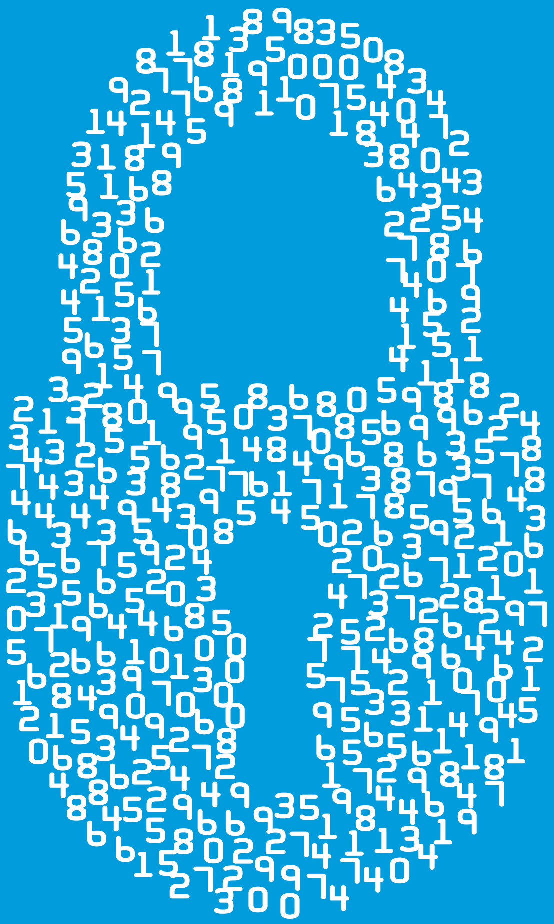
KPMG

Achieving Digital Forensic Readiness

Prepare – Partner – Evolve



kpmg.com.au

Achieving Digital Forensic Readiness

You can probably still recall the last digital incident that hit your organisation, such as ransomware encrypting your important documents, internal fraud in your finance department or a hacker detected by your security monitoring solution.

During this incident, did you know which internal and external stakeholders to call, and did you have a message prepared? Were you able to quickly preserve the data and log files from your systems? And how about the log files from your incident response providers and cloud solutions? Were your incident response team members prepared for their roles? Were they aware of what, when, where and how to deal with the incident?

When dealing with a digital incident in your organisation, it is essential to stay in control of the situation. You want to be able to respond from a position of strength, not be driven by panic. Despite many examples to the contrary and perhaps your own experience, our message is that you can. You can regain control over digital incidents by working on Digital Forensic Readiness – the state in which you are properly prepared to handle digital incidents.

Why should I aim for Digital Forensic Readiness?

Digital incidents are a fact of life for many large companies. 100 percent security is never feasible, and aiming for it is not sensible from a business perspective.

Instead, you deal with digital threats as with many other risks to your business, like fires or a disruption in your supply chain. Of course, prevention is crucial. But so is being able to deal with incidents once they do occur.

That ability is what we call Digital Forensic Readiness.

What is Digital Forensic Readiness?

Digital Forensic Readiness allows you to regain control, and limit the damage and costs from a digital incident.

Our vision for Digital Forensic Readiness builds on three building blocks: **preparing**, **partnering** and **evolving**. With these building blocks, you create a well-oiled machine that is ready to kick-in when a digital incident occurs. Instead of improvising your way through, responding to such incidents becomes a matter of following a carefully shaped playbook with a prepared team.

In the remainder of this document we discuss these building blocks of Digital Forensic Readiness, and what it takes to achieve it.

Prerequisites for Digital Forensic Readiness

Being able to effectively deal with incidents once they occur requires preparation and a certain level of maturity in your organisation. For example, it is crucial that you have already developed detection and response fundamentals: you have implemented security monitoring and have incident response teams in place.

This is the starting point for building Digital Forensic Readiness in your organisation.

The three components of Digital Forensic Readiness

In our view, building a forensic-ready organisation requires attention to three main aspects: preparing, partnering, and evolving.

1 / Preparing

You cannot plan for the next cyber incident, but you can make sure that you are prepared when it does happen. Being prepared requires you to create and maintain the conditions that enable a timely and effective response to a digital incident. A crucial ingredient for this is a playbook: the primary reference document on how your organisation will deal with digital incidents.

Furthermore, it must be clear that creating Digital Forensic Readiness is not a one-off exercise that can be delegated to a small team of specialists. Being prepared requires a sustained effort from various parts of your organisation, not only IT but also communication or legal team. A second common misconception is the idea that Digital Forensic Readiness is primarily a technological issue. In our view people and processes are at least equally important.

When preparing for digital incidents, the following aspects should be considered:

- **People**
  Who has the mandate to take the critical decisions during an incident? Do we have the people available with the right training, skills and experience?

- **Processes**
  Have we outlined the steps we need to go through when digital incidents occur? Are essential processes around incident response defined, such as investigation, escalation, eradication, recording the audit trail and reporting on progress? Is it clear how internal and external communications should occur during an incident?

- **Technology**
  Do we have the required tools available to adequately analyse data? Are we able to retrieve the right data? In what physical location is data stored, and are there any legal obstacles to retrieve it? If e-mail runs in the cloud, will our providers supply us with the log files we require?

Playbook: recipe for a successful response

The steps to take in response to a digital incident should be recorded in a playbook. When preparations have been done properly, your playbook will offer guidance during digital incidents such that your team knows who should do what, how and when.

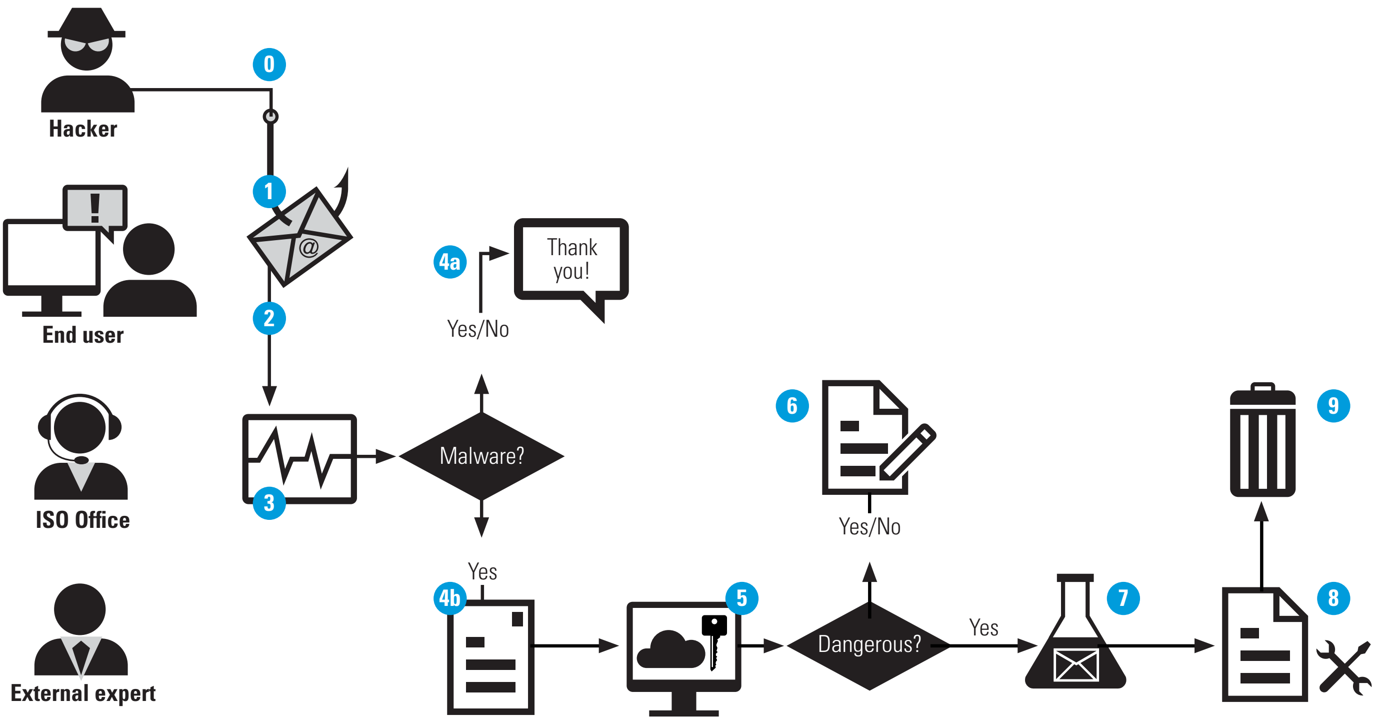
Typically, such a playbook involves a number of reference elements:

- Team roles, responsibilities, escalation guidelines and contact details.
- Communication channels.
- Initial response procedures, such as safeguarding relevant data.
- Investigative procedures and countermeasures.

Furthermore, the playbook provides guidance on how to approach a new digital incident. This entails, amongst others:

- Agreeing on the preliminary goal: what exactly do we want to know and what do we investigate?
- Getting started: assign key roles, timelines, internal and external communication channels.
- Containing/isolating compromised network sections where needed.
- Increasing security and monitoring for critical sections of the infrastructure – your crown jewels.
- Updating detection systems based on findings.
- Eradication: Do we want to follow a hacker within our network or do we deny him access?
- Ongoing evaluation of progress and capabilities and mobilising external parties where needed.

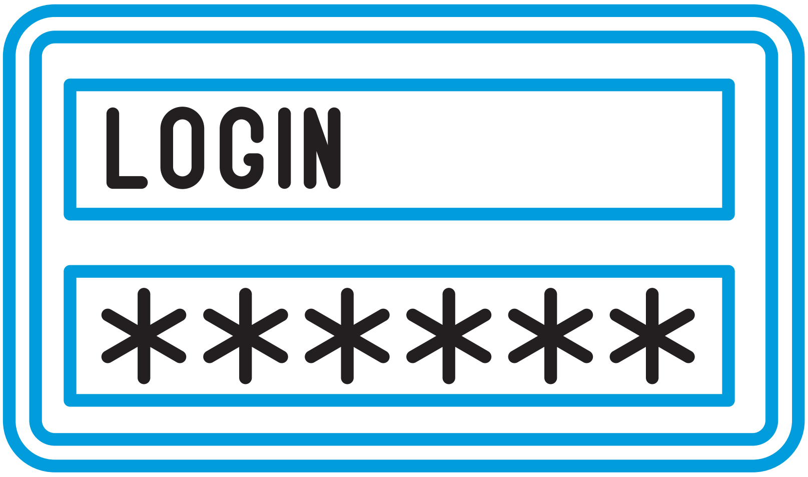
Example: **Anatomy of a digital incident**



0. Hacker sends phishing mail
1. Potential phishing received
2. Notify the ISO Office
3. Perform first analysis

4a. Feedback notifier
4b Escalate to external expert
5. Run phishing mail in standalone sandbox
6. Send report

7. Run malware in malware laboratory
8. Build malware wiper
9. Send malware wiper



2 / Partnering

There are many good reasons to forge relations with external specialists and stakeholders when it comes to dealing with digital incidents.

- Dealing with digital incidents often requires expertise which is not readily available within your own organisation.
- Moreover, during digital incidents there are various external parties which need to be communicated with, such as regulatory authorities and potentially law enforcement.
- Lastly, if you are an international organisation you must be able to call on local experts and backup worldwide.

A sustained effort is needed here as well, partnering is not only about establishing the initial contacts with the relevant stakeholders. Digital Forensic Readiness requires that these relations are developed into true partnerships. There is an important but often overlooked 'soft' element to that. Introductions are best made before a crisis emerges, so that the internal incident response team and the external provider work together seamlessly. It really helps if those in the frontline are already familiar with one another from previous joint exercises or other interactions.

3 / Evolving

By learning from your own organisation and from others, you can evolve your organisation and thereby improve your Digital Forensic Readiness both reactively and proactively.

It is unlikely that a particular type of digital incident occurs in your organisation for the first time ever. It is probable that one of your peers has dealt with a similar incident before. Therefore, it pays off to learn from others. With that of course, comes the need to reciprocate and share your own experiences.

In addition to learning from others, your organisation needs to learn by itself as well. Periodic rehearsing, evaluating and updating your playbook are essential parts of Digital Forensic Readinesss.

In summary, there are three important components to evolving in the area of Digital Forensic Readiness:

1. **Periodic sharing of information**
   about emerging threats, attack patterns, best practices and defensive tactics with your peers, and discussing results of security testing and changes in your IT landscape with your forensic partners.
2. **Incident response exercises**
   Practice drills with simulated incidents in your production environment (both planned and unannounced) and table top exercises, such as cyber war games. These exercises should also involve external partners, e.g. IT suppliers and data storage facilities.
3. **Evaluating incident response and drawing lessons from actual incidents**
   How adequate were procedures, and where did issues occur? How useful was the playbook, and where does it require updates? How do we share and deploy the lessons learned to other parts of the organisation?

Importance of external relations

The impact of a digital incident often extends well beyond your organisation and could affect many stakeholders and your supply chains. Could the incident have a material impact on financial statements? If so, the external accountant, the investor relations department, regulatory authorities and a host of other stakeholders will need to get involved. If there is a criminal intent behind the incident, it helps to have the right contacts with the relevant law enforcement agencies, the Australian Cybersecurity Centre (ACSC), etc. Also, consider the effect of the draft bill on mandatory data breach disclosures.

Furthermore, adequately dealing with digital incidents often requires expertise that may not be readily available within an organisation. For example, extracting data from cloud systems or investigating hacker attack patterns.

It pays off to know the right people and to already have contracts in place. You do not want to waste time looking for experts and discussing fees in a time of crisis.

When an incident occurs

In a state of Digital Forensic Readiness, dealing with digital incidents has become 'business as usual' for your organisation. Your response plans have been thoroughly rehearsed, evaluated and fine-tuned, in tandem with your external partners and stakeholders.

When the next digital incident happens, you are ensured that it will be dealt with effectively and efficiently. Right from the start, the incident response team convenes quickly and gets down to business. They act in a calm and confident manner. Everybody on the team knows precisely what to do since they have gone through the playbook many times. Collecting all the necessary data is not a problem, not even for your data that is stored in the cloud. Great care is taken to keep all stakeholders up to date of the latest developments. They can feel confident too, knowing that all preparations are paying off and the incident is being handled in the best possible way.

Whatever comes your way, there will be no surprises. Costs and damage from the incident are kept to a minimum. You have achieved Digital Forensic Readiness. You will remain in control.

KPMG Australia's team of high-performing cyber security advisors and digital forensic experts are available to help you achieve Digital Forensic Readiness.

Contact

Martin Dougall
Partner, Forensic
+61 392 885 511
mwdougall@kpmg.com.au

kpmg.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

October 2016. NSW N14690ADV