



ACHIEVING DIGITAL FORENSIC READINESS

Prepare-Partner-Evolve

ACHIEVING DIGITAL FORENSIC READINESS

You can probably still recall the last digital incident that hit your organization, 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 story prepared? Were you able to quickly collect the data and log files from your systems? And how about the log files from your providers and cloud solutions? Were your 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 organization, 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 through achieving Digital Forensic Readiness – the state in which you are properly prepared to handle upcoming digital incidents.

Why should I aim for Digital Forensic Readiness?

Digital incidents are a fact of life for many large companies. 100% 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 there. 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 organization. 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 organization.

THE THREE BUILDING BLOCKS OF DIGITAL FORENSIC READINESS

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

1 / PREPARING

Of course you cannot plan when the next incident is going to happen, but you can make sure that you are prepared when it does. Being prepared requires that you create and maintain the conditions that enable you to respond timely and effectively to any digital incident. A crucial ingredient for this is a so-called playbook: the primary reference on how your organization wants to 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 organization, not only IT but also communications, legal, etc. A second common misconception is the idea that Digital Forensic Readiness is primarily a technological issue. In our view the dimensions people and processes are 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 and certifications?
- **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? Do we have a war room prepared? Is it clear how internal and external communications should function 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 my data stored, and are there any legal obstacles to retrieve them? If e-mail runs in the cloud, will our providers supply us with the log files we require?

PLAYBOOK: RECIPE FOR A SUCCESSFUL RESPONSE

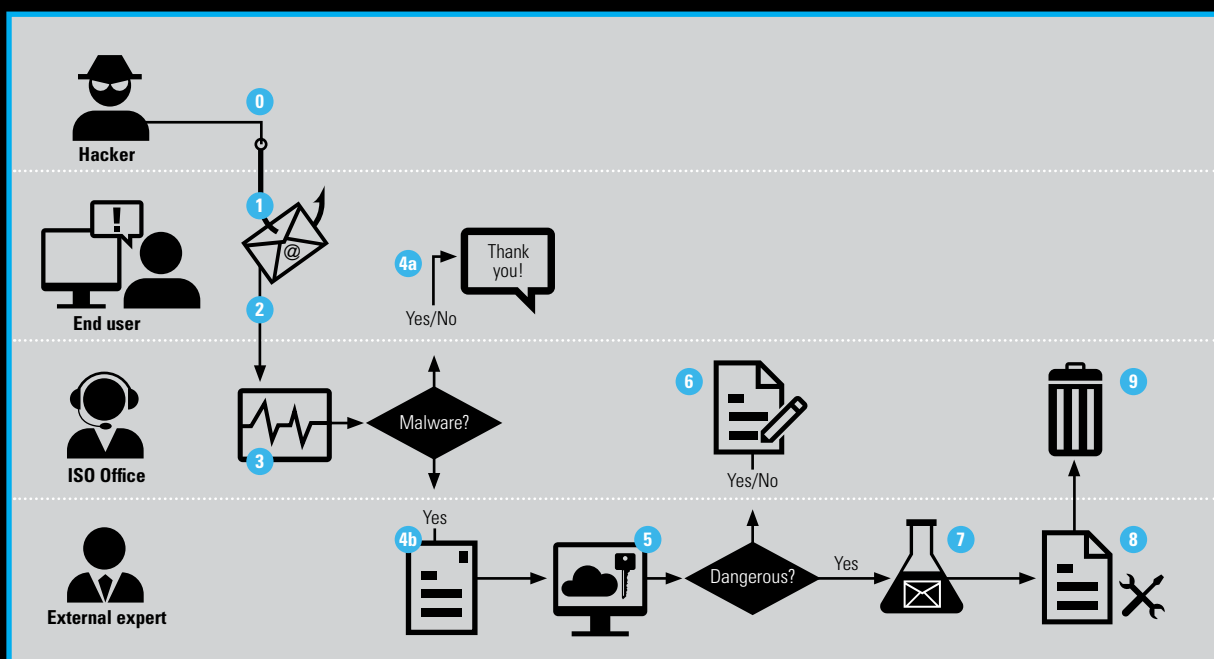
The steps to take in response to a digital incident should be recorded in a playbook. When preparations have been done properly, your playbook will offer guidance during digital incidents such that your team knows who should do what, how and when.

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 kick him out immediately?
- Ongoing evaluation of progress and capabilities and mobilizing external parties where needed.



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 and 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 organization.
- Moreover, during digital incidents there are various external parties which simply cannot be overlooked, such as regulatory authorities and law enforcement.
- Lastly, if you're an international organization you must be able to call on local experts and backup worldwide.

Here as well a sustained effort is needed: 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. You don't want people to have introduced themselves to each other during a crisis. It really helps if those in the frontline are already familiar with one another from previous joint exercises or social events.

3 / Evolving

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

It is unlikely that a particular type of digital incident first occurs in your organization. It is probable that one of your peers has dealt with a similar incident before. Therefore, it pays off to open up to the world and be willing 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 organization needs to learn by itself as well. Periodical rehearsing, evaluating and updating your response plan are essential parts of digital forensic readiness.

In summary, there are three important elements in evolving in the area of digital forensic readiness:

- **PERIODICAL 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.

- **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.

- **EVALUATING INCIDENT RESPONSE AND DRAWING LESSONS FROM ACTUAL INCIDENTS:**

How adequate were procedures, and where did hiccups 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 organization?

Importance of external relations

The impact of a digital incident often extends well beyond your organization and could affect many stakeholders. 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 (usually not the police station around the corner), the National Cybersecurity Center (NCSC), etcetera.

Furthermore, adequately dealing with digital incidents often requires expertise that may not be readily available within an organization. For example consider 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 the experts and discussing fees in crisis time.

IN CASE AN INCIDENT OCCURS

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

So for your next digital incident to happen, 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 nasty surprises. Costs and damage from the incident are kept to a minimum. You have achieved Digital Forensic Readiness. You will remain in control.



KPMG NETHERLANDS IS A RECOGNIZED MARKET LEADER IN CYBER SECURITY AND FORENSIC INVESTIGATIONS. OUR TEAM OF 60+ HIGH-PERFORMING CYBER SECURITY ADVISORS AND DIGITAL FORENSIC EXPERTS ARE AVAILABLE TO HELP YOU ACHIEVE DIGITAL FORENSIC READINESS.

Contact

John Hermans

Partner, Risk Consulting

E: Hermans.John@kpmg.nl

T: +31 6 5136 63 89

Hans Wim Tinholt

Manager, Risk Consulting

E: Tinholt.HansWim@kpmg.nl

T: +31 6 21393598

Jeroen de Wit

Senior Consultant, Risk Consulting

E: deWit.Jeroen@kpmg.nl

T: +31 6 46748584

kpmg.com/nl/cybersecurity

© 2015 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ('KPMG International'), a Swiss entity. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor 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.