Cyber Forensic Readiness: An Integrated Approach

Adv Jacqueline Fick
PwC: Forensic Technology Solutions
Agenda

- Cybercrime: What statistics have shown
- Key trends that impact on the environment organisations operate in
- What is cyber forensic readiness?
  - Cyber forensic readiness defined
  - Why do organisations need to be ‘cyber incident ready’?
  - What happens to the potential evidence prior to the decision to undertake an investigation?
  - Managing the risks: why digital evidence and potential disputes are important
  - Why should organisations be concerned about cyber forensic readiness?
- Key questions to ask
- Closing remarks
“In a world where cyber crime is constantly increasing, pervasive computing is on the rise and information is becoming the most sought after commodity making an effective and efficient Information Security architecture and program essential. With this improved technology and infrastructure, ongoing and pro-active computer investigations are now a mandatory component of the IS enterprise. Corporate governance reports require that organizations should not only apply good corporate governance principles, but also practice good IT governance and specially IS governance. Organizations develop their security architectures based on current best practices for example ISO 17799 and COBIT. These best practices do not consider the importance of putting controls or procedures in place that will ensure successful investigations. There is a definite need to adapt current IS best practices to include for example certain aspects of Digital Forensics readiness to the current best practices to address the shortcomings.”

(Grobler and Louwrens Digital Forensic Readiness as a Component of Information Security Best Practice)
Cybercrime: What statistics has shown

- Cybercrime: Protecting against the growing threat (PwC Global Economic Crime Survey, November 2011)
- Organisations face serious internal and external threats from cyber criminals.
- Cybercrime now ranks as one of the top four economic crimes.
- Cyber security issues now top the list of risks to watch, ahead of weapons of mass destruction and resource security. (World Economic Forum Global Risks 2011 report)
- Traditionally leaders have pigeonholed cyber security as an IT problem. But that is a risk approach that could leave them open to attack.
Reputational damage is the biggest fear for 40% of respondents

Two in five respondents had not received any cyber security training

60% said their organisation doesn’t keep an eye on social media sites

A quarter of respondents said there is no regular formal review of cybercrime threats by the CEO and the Board

Four in ten respondents say that their organisation does not have the capability to prevent and detect cybercrime

The majority of respondents do not have, or are not aware of having a cyber crisis response plan in place
<table>
<thead>
<tr>
<th>Macro-economic, Social and Business Drivers</th>
<th>Infrastructure Revolution</th>
<th>Data Explosion</th>
<th>Always-on, Always-connected world</th>
<th>Mobile device explosion</th>
<th>Tougher regulation and standards</th>
<th>Life in the cloud</th>
<th>New identity and trust models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Globalisation</strong></td>
<td>• Increase in availability of high speed broadband and wireless networks</td>
<td>• Greater sharing of sensitive data between organisations and individuals</td>
<td>• Greater connectivity between people driven by social networking and other platforms</td>
<td>• Increasingly seamless connectivity between devices</td>
<td>• Broader legislative and regulatory oversight</td>
<td>• Widespread adoption of cloud-based services in a drive to cut infrastructure and administration costs</td>
<td>• Identity becomes increasingly important in the move to information based security</td>
</tr>
<tr>
<td><strong>Changing workforce demographics and diversity</strong></td>
<td>• Blurring work/personal life divide</td>
<td>• More people connected globally</td>
<td>• Increasing information and data mining</td>
<td>• ‘Bring Your Own’ approach to enterprise IT</td>
<td>• Increasing standards on Information Management and Governance</td>
<td>• New models of trust for people, infrastructure and data emerge</td>
<td></td>
</tr>
<tr>
<td><strong>Increasing regulation</strong></td>
<td>• Content rich data – video, audio</td>
<td>• A multiplication of devices and applications generating traffic</td>
<td>• Increased Critical National Infrastructure and public services connectivity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Expectations of demonstrable governance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rapid technology innovation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Changing attitudes to privacy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber forensic readiness is the organisations’ potential to maximise the use of digital evidence to aid in an investigation, with the intent of:

- Reducing the time taken to respond to an incident.
- Maximising the ability to collect credible and meaningful evidence.
- Minimising the length/cost of a cyber incident investigation.
- Reducing the incident recovery time.
- Preventing further losses.
HoneyNet Project

- The HoneyNet project shows that the average time spent in a cyber investigation was approximately 34 hours per person to investigate an incident that took an intruder about half an hour. That's about a 60:1 ratio!

(http://www.honeynet.org/challenge/results/index.html)

(William Beer, Director, Cyber Security Services, PwC UK)
A reactive or tactical approach to Information Security may introduce significant costs and opportunity loss.
Why do organisations need to be ‘cyber incident ready’?

- Digital forensic investigations (DFIs) are commonly employed as a post-event response to a serious information security or criminal incident.
- The examination is conducted in a systematic, formalised and legal manner to ensure the admissibility of the evidence and subject to considerable scrutiny of both the integrity of the evidence and that of the investigation process.
- There is a broad organisational role in the forensic readiness process. This role can be equated to a business continuity process.
People

Processes

Technology

Governance

Cyber Forensic Readiness Plan
What happens to the potential evidence prior to the decision to undertake an investigation?

- The scenario of a DFI tends to ignore what happens to potential evidence prior to the decision to undertake an investigation.
- The necessary evidence either exists, and hopefully is found by the DFI, or it does not exist and a suspect cannot be charged and prosecuted.
- When a digital incident occurs there are generally three courses of action that can be taken, generally dependant on the type of organisation within which the incident occurs, or which is responding the event:
Law Enforcement

- Secure the crime scene, identify evidentiary sources and dispatch to a specialist laboratory for analysis.

Military Infrastructure

- Primary goal is one of risk identification and elimination, followed by recovery and possible offensive measures.

Commercial Organisations

- Where financial impact is caused by an incident, and revenue earning potential is adversely affected, root cause analysis and system remediation is of primary concern, with in-depth analysis of the how and why left until systems have been restored.
• The business environment lends itself to an approach similar to that of the military, namely to be able to identify the incident, patch the necessary system(s) and continue earning revenue.
• In the generic (law enforcement) investigative model, there is little leeway for a business’s incident responders to satisfy the need to return the systems to operational status as quickly as possible whilst preserving the necessary evidence and being able to mount a successful prosecution.
• These two goals can be mutually exclusive as a thorough investigation needs time and during this time the business will lose revenue by not having its system(s) live.
Managing the risks: Why digital evidence and related disputes are important

Recourse to litigation is generally a last resort for most organisations, but digital evidence could help manage the impact of some important business risks:

- Lend support to internal disciplinary actions
- Support a legal defence
- Support good IT governance practices and reporting
- Show that due care (or due diligence) was taken in a particular process
- Support a claim to intellectual property rights
- Verify the terms of a commercial transaction
• Being prepared to gather and use evidence can also act as a deterrent. Staff will know what the organisation’s attitude is toward the policing of corporate systems – how incidents are dealt with and how the organisation deals with offenders.
• This also highlights the need for internal policies and procedures that are communicated via effective awareness and training programmes throughout the organisation.
• Staff need to know:
  ✓ Who the perpetrator could be and what to look out for?
  ✓ What can be done?
  ✓ Who to call?
For most organisations the foremost objective is not to secure evidence. It is more important to find the offender, locate the intruder, and more importantly secure the infrastructure by minimising, or if possible, eliminating vulnerabilities.

To ensure that the organisation maintains a pro-active approach it is of great value to conduct simulated cyber incident exercises. This would also facilitate a process of continuous learning and awareness.

Cyber forensic readiness claims that the time and cost required for an incident response during a digital forensic investigation should decrease while at the same time maintaining the level of credibility of the digital evidence being collected. Time = money.
### Key questions to ask

<table>
<thead>
<tr>
<th>Question</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you know if you are able to handle a cyber crime incident and are you able to adapt to the fast pace and new emerging risks of this type of crimes?</td>
<td>Do you know where your threats are most likely to come from?</td>
</tr>
<tr>
<td>How often is your staff trained on cyber security?</td>
<td>Do you know the security posture of their systems?</td>
</tr>
<tr>
<td>Do you have current knowledge of emerging cyber threats?</td>
<td>Are your policies aligned with the regulatory and legislated requirements?</td>
</tr>
<tr>
<td>Do you maintain a proper chain of evidence?</td>
<td>Do you know what information is required to carry out an investigation?</td>
</tr>
<tr>
<td>Do you know what an attack signature will look like?</td>
<td>Are you able to carry out an investigation?</td>
</tr>
<tr>
<td>Do you have centralised and secure logging facilities?</td>
<td>Do you know who to call and what to do when an incident has occurred?</td>
</tr>
<tr>
<td>Do you know your high risk systems?</td>
<td>Are you aware of the legal requirements around the handling of evidence?</td>
</tr>
</tbody>
</table>
Closing Remarks

• Being ready for a forensic investigation should form part of any information security strategy.
• It is also closely related to incident response and business continuity, ensuring that evidence found in an investigation is preserved and the continuity of evidence is maintained.
• Get in the experts: take a detailed look at the organisation's readiness to undertake or support a digital forensics investigation, be this as part of an internal investigation, criminal investigation or as the result of a compliance requirement.
• Cyber forensic readiness plans should take cognisance of people, processes, technology and governance aspects.
• What needs to be done:
Define the business scenarios that will require digital evidence. When it will be appropriate to gather evidence and when is it not?

Identify sources of evidence and what type of evidence it is, and ensure that you have the resources available to look for it.

Establish a clear view of what circumstances need to be in place to trigger a full investigation.

Provide guidance in the preparation of an example that everyone can run through in advance. Ensure that all parties, including legal, are confident that the correct processes are in place.

Provide training for key staff to ensure that evidence handling procedures are adhered to.

Create learning organisations. Assess the adequacy of the investigation and the utility of the evidence gathered to support it. Incorporate in cross-departmental training initiatives to create and maintain staff awareness across the organisation.

Develop policies and procedures to ensure compliance.
Questions?