Orion Investigations
20th Floor, Unit 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

Why is Computer Forensics Important to Your Organisation?

February 2012

Date: 02-02-2012

Author: Andrew Smith

Contents

About the Author

Andrew Smith – Director of Computer Forensic Services, Orion Investigations

Andrew is responsible for the management of the Orion Computer forensic Unit. His responsibilities include ensuring the unit operates to the highest international standards, business development and the development and delivery of training for clients and staff. Andrew is an experienced forensic investigator with extensive training and comprehensive experience in relation to criminal, corporate, malware and counter terrorism investigations within the UK and Europe. He has worked in the public sector with the South Yorkshire Police where he received his initial training in computer forensics and also in the private sector with a leading UK computer forensics company. He is also an experienced trainer having developed UK Law Society approved training courses and delivered master degree level forensic training. With nearly ten years' experience in the field of computer forensics Andrew has regularly appeared in court as an expert witness to present complex computer evidence.

Introduction

In today's fast paced world, organisations have to rely more and more heavily on technology to remain competitive. Customers have come to expect organisations to have an online presence with professional looking websites, be able to respond quickly to online enquiries, have online chat functionality and have the ability to order online.

Technology has become so integrated into people's lives that they expect to have constant access to their personal emails and to be able to stay in touch with friends even during working hours.

What does this mean for organisations? It means that they will face some kind of cyber-security incident and the reality is they are often unprepared to deal with the incident effectively.

Organisations are aware they need to have firewalls in place, up to date anti-virus and the latest patches installed. However they often do not enforce their acceptable computer usage policy or give any thought to the control of USB devices that can be plugged into the network or mobile phones that may hold company data. In addition when an employee's contract is terminated the organisation often overlooks the need to quickly close down the employee's user accounts which can include remote access to the network.

Organisations have a legal and moral obligation to protect their customer's personal information however data leakage remains one of the biggest problems they face in todays' technological world.

Cyber-Security Incidents

Every organisation will eventually have to deal with a cyber-security incident in one form or another. Examples of cyber-security incidents include

- Computer fraud.
- Criminal activities.
- Industrial espionage.
- Theft of proprietary corporate data/information.
- Privacy act violations/customer data loss.

- Child pornography, adult pornography.
- Violations of organisational computer security policies and more.

When such an incident occurs it can leave the organisation in a vulnerable position, ethically, financially and legally. All incidents need to be treated seriously. What starts out initially as an internal investigation could quickly expand into a criminal investigation which then involves outside agencies or the investigation could leak out to the public or the media.

Highlights from the 2011 Global Economic Crime Survey

- Cybercrime now ranks as one of the top four economic crimes.
- Reputational damage is the biggest fear for 40% of respondents.
- 60% said their organization doesn't keep an eye on social media sites.
- 34% of respondents experienced economic crime in the last 12 months (up from 30% reported in 2009).
- Almost 1 in 10 who reported fraud suffered losses of more than US$5 million.
- 56% of respondents said the most serious fraud was an 'inside job'.
- 2 in 5 respondents had not received any cyber security training.
- The majority of respondents do not have, or are not aware of having, a cyber-crisis response plan in place.

Why is Computer Forensics Important to your Organisation?

When a cyber-security incident occurs the IT staff will often be expected to make an initial assessment to try and identify the exact nature and seriousness of the incident. They will often not have received any kind of computer forensic training. As a result they are not necessarily aware of the issues surrounding the collection of digital data that may have to be relied upon at a later date in court. Vital information such as time and date stamps can be lost making the investigation more difficult. In the

worst case scenario vital evidence may be thrown out of court due to the improper handling of the data during the course of the investigation.

Computer forensic investigations require specialist skills which involves not just the preservation and identification of digital evidence but the correct interpretation of that evidence. When confronted with a forensic investigation, organisations initially tend to focus on the costs involved. Yes there is an up-front cost and depending on the complexity of the investigation and the number of computers involved, it can appear to be expensive. However consider the following:

- Evidence that can only be obtained by a forensic examination can often prove vital to the successful outcome of the investigation.
- A forensic investigation can often reduce the need for full legal action to be taken.
- A forensic investigation can save time resulting in a saving of money.

When formulating an incident response plan, organisations should be building into that plan a forensic response. This may mean providing staff with computer forensic training, identifying computer forensic companies with the skills already that can assist, or a combination of both.

Computer forensics is now well established in many countries around the world and is rapidly gaining momentum in many other countries. In the UK they have now even set up an insurance scheme where if the organisation is required to call in a computer forensic company, they can claim it on insurance. Organisations need to embrace forensics and use it as another tool against those who are committing cyber-crime.