

Countering Cyber Crime:

It's Everyone's Responsibility

IP

A Special Report By International Perspectives
www.internationalperspectives.org

Table of Contents

Overview & Highlights	2
The Problem: Avoiding Responsibility	4
The Cause: Defining Cyber Crime	6
Measures For Individuals	7
Parents	11
Educators	12
Employees	14
Measures For Organizations	15
Business	15
Industry	17
Law Enforcement	18
Government	20
Future Considerations	23
Conclusion	25
Glossary of Terms	27
Further Interest	29

Disclaimer

This International Perspectives report contains analysis of perspectives and issues related to cyber crime. As such, this report is to be used for general reference purposes only and is not to be construed as legal advice.

This report is copyright © 2007 International Perspectives and may not be reproduced, duplicated or distributed beyond the purchaser of this report. All rights reserved. IP#

Overview & Highlights

Overview:	<p>Due to a widespread lack of understanding on the topic, many have been slow to accept responsibility for countering cyber crime. This report considers the countering of cyber crime from a perspective geared at increasing awareness among a non-technical audience. In doing so, recommendations consisting of simple ways in which individuals and organizations can effectively counter cyber crime are made. Drawing from discussions held at a closed workshop on cyber crime, this report builds on the opinions of experts from a variety of fields.</p>
Who Should Read This?:	<p>Anyone with a vested interest in countering cyber crime, particularly, those readers looking to understand an oft-intimidating topic from a non-technical perspective or those responsible for disseminating an understanding on the topic to a non-technical audience.</p>
Note on the Text:	<p>Hyperlinks are provided to source material throughout the body of the text. As a result, the report is best read at a computer connected to the Internet.</p>
Highlights	<ul style="list-style-type: none">• Simple Steps can counter cyber crime, but everyone must play their part. Anyone using Information Communications Technology is responsible for the prevention of cyber crime. Accepting responsibility is as basic as keeping Personal Computer software up-to-date or being cautious about sharing private information.• Nearly half of all experts polled felt a lack of understanding most hinders cyber crime counter measures. A shift in focus from the technology involved in cyber crime onto the criminal act itself will increase awareness among non-technical people, encouraging uptake of simple yet effective counter measures.• Education around issues in cyber crime and security must be increased. From the elementary to graduate levels, new programs need to be implemented and existing ones reassessed. Introducing mandatory courses on computer ethics at the introductory level and emphasizing the need to integrate security into software development at higher levels are absolutely necessary to counter cyber crime in the long-term.• The Security industry should be prepared for a permanent shift towards openness regarding personal data among the average user. Although strong awareness campaigns can help discourage user disclosure of sensitive information, current trends suggest that the preponderance among average users to reveal personal information does threaten traditional identity-based approaches to security.

Countering Cyber Crime:

It's Everyone's Responsibility

Rates of cyber crime have been increasing at an alarming speed. In part, cyber crime continues to spread due to a growing use of information communication technology (ICT), which plays an ever-important role in our daily lives. Individuals and organizations, however, which tend to typically be the victims of such illicit activity, are also playing a part in the effective spread of cyber crime. For many people, forming an understanding of what cyber crime really is has proven elusive. This lack of familiarity with the topic has led many to do nothing to counter the threat, under a misguided belief of not being responsible, thereby unwittingly abetting criminals. Considering the barriers to forming a working understanding of cyber crime, this report provides simple measures and ideas which even the non-technical reader can implement to counter the threat.

The Problem: Avoiding Responsibility

As quickly as ICT products have flooded the market and entered our lives, cyber crime rates have risen - perhaps at an even faster rate. Criminals have found a prime environment for conducting illicit activity in a digital world, while law abiding segments of society continue to grapple with developing an understanding of what cyber crime really is. The inability to comprehend the problem has left many with a sense of not being responsible for actively countering the threat.

This avoidance of responsibility plagues individuals, industry, corporations and governments alike. Stemming from a lack of understanding brought on by a broadness of definition, decision makers are paralysed when faced with the task of developing practical measures to counter cyber crime. Instead of actually taking steps to counter cyber crime, many opt to shift the responsibility, and ultimately blame, onto someone or something else. Such irresponsibil-

ity can manifest itself in individuals who store user passwords on notepads beside desktop computers to companies marketing products as completely secure when that is not the case to politicians who ignore the topic due to a lack of understanding.

The economic consequences of avoiding responsibility are considerable. Following a data breach in one of its stores, The TJX Companies Inc. spent US\$12 million in the first quarter of fiscal 2008 alone on investigations into the network intrusions said to have occurred in 2005 and 2006. These costs are to say nothing of the prolonged financial losses that might be sustained including pending and potential law suits as a result of the breach. Breaches of customer or user data can affect millions of people, often putting sensitive personal information such as credit card and social insurance numbers into the hands of criminals – resulting in many unhappy, at-risk customers, leading to more unhappier investors.

