# CYBERCRIME: FROM PREVENTION TO PROSECUTION

<table>
<thead>
<tr>
<th>Date</th>
<th>24 February 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Venue</td>
<td>Crowne Plaza Hotel, Ortigas Center, Quezon City</td>
</tr>
</tbody>
</table>

## Training Details:
CPE Units: 8  
Basic level

## Agenda:

### Investigating Cybercrime Incidents
When a cybercrime occurs – or worse, when it is discovered after the fact, your organization will need to find out exactly what happened. This session will discuss available investigation techniques necessary to guide and manage that process. It will present digital forensic tools and procedures to analyze networks to recreate the steps making up the cybercrime event. Our speakers will talk you through the science and art of preserving digital evidence, and establishing a chain-of-custody to ensure the integrity of electronic evidence for purposes of litigation and prosecution.

[DREXX D. LAGGUI](#)  
CISA CISSP CCSI CSA  

[MARIO B. DEMARILLAS](#)  
CFE COBIT (F) CRISC CISA CISM CIA CPA  
Board of Trustee, Association of Certified Fraud Examiner Philippines & ISACA Manila Chapter

### Enhancing Interviewing Skills for Investigation
Many security experts say that people are the weakest link in the security chain. This explains the continuing power of social engineering and its leading role in the commission of cybercrimes. Getting accurate information from the persons involved in the event is crucial in establishing a sequence of events and is therefore helpful in prosecuting cybercrimes. More importantly, human weaknesses reveal security vulnerabilities in your organization. The ability to read verbal cues and body language is crucial in these situations. In this session, our speaker will discuss these techniques to enhance your interviewing skills to spot the liars from the truth-tellers. These will greatly aid in your own cybercrime investigations.

[JONATHAN DAVISON](#)  
Managing Director  
Forensic Interview Solutions (FIS) Ltd.

### Keynote: The Office of Cybercrime Initiatives
The recently issued Implementing Rules and Regulations (IRR) for the Cybercrime Prevention Act spells out the specific roles of various government agencies in combatting cybercrimes. The central authority is the Office of Cybercrime housed in the Department of Justice (DOJ). Our keynote speaker, Hon. Emmanuel Caparas, will provide an overview of the DOJ’s efforts and present the plans of the Office of Cybercrime for 2016.

[HON. EMMANUEL CAPARAS](#)  
Undersecretary  
Department of Justice and Chief Office of Cybercrime

### Cybercrime Law Enforcement Panel
This session features the primary law enforcement agencies tasked with investigating cybercrimes and apprehending violators of the Cybercrime Prevention Act. Both the PNP and NBI will discuss past cases and identify the current trends in local and cross-border cases. They will also feature the services they provide to victims and complainants including digital forensics, surveillance, raids, arrest and preparation of initiatory documents for the prosecution of offenders.

[Philippine National Police & National Bureau of Investigation](#)
### Cybercrime Updates: The IRR of the Cybercrime Prevention Act

After the Supreme Court for the most part, upheld the validity of the Cybercrime Prevention Act, the government issued the Implementing Rules and Regulations. This session will discuss those developments as well as the challenges of prosecuting cybercrime cases.

**ATTY. JJ DISINI**
Managing Partner, Disini & Disini Law Office

### Emergency Response to Cybercrime Events

Cybercrime emergency requires interventions in different domains. Many questions arise in the midst of an on-going emergency. What should we do? Should we shut down? Should we disconnect from the Internet? What do we tell our employees to do? How to we minimize damage or prevent further damage? How should we handle this internally and externally? This session will present best practices in the field of emergency response and will aid participants in striking a balance between defending the network and minimizing damage to your infrastructure and reputation.

**ALBERT DELA CRUZ**
Director, Philippine Computer Emergency Response Team

### Preventing Cybercrimes

Benjamin Franklin famously said “An ounce of prevention is worth a pound of cure.” Recent hacks have certainly demonstrated that. The famous Sony Pictures hack cost the company $35M in IT repairs and untold losses in reputational costs. Sony even paid its employees $8M to settle claims arising from the breach of personal privacy. The US retailer, Target, was the victim of a data breach that resulted in out-of-court settlements to its customers and Visa in the amount of $10M and $67M, respectively. This session aims to provide practical tips to secure your network, identify the weak links in your security chain, and identify interventions that can aid in improving your efforts at avoiding a cybercrime event in your organization.

**HENRY AGUDA**
Chief Technology and Information Officer
Amihan Group

---

Crowne Plaza Hotel, Ortigas Center, Quezon City, February 24, 2016

**AGENDA**

**Investigating Cybercrime Incidents**

**Mr. Drexx Laggui,** Principal Information Security Consultant, Laggui & Associates, Inc.

**Mr. Mario Demarillas,** Board of Trustee, Association of Certified Fraud Examiner Philippines & ISACA Manila Chapter

_When a cybercrime occurs – or worse, when it is discovered long after the fact, your organization will need to find out exactly what happened. This session will discuss available investigation techniques necessary to guide and manage that process. It will present digital forensic tools and procedures to analyze networks to recreate the steps making up the cybercrime event. Our speakers will talk you through the science and art of preserving digital evidence, and establishing a chain-of-custody to ensure the integrity of electronic evidence for purposes of litigation and prosecution._

**Enhancing Interviewing Skills for Investigation**

**Mr. Jonathan Davison,** Managing Director, Forensic Interview Solutions (FIS) Ltd.
Many security experts say that people are the weakest link in the security chain. This explains the continuing power of social engineering and its leading role in the commission of cybercrimes. Getting accurate information from the persons involved in the event is crucial in establishing a sequence of events and is therefore helpful in prosecuting cybercrimes. More importantly, human weaknesses reveal security vulnerabilities in your organization. The ability to read verbal cues and body language is crucial in these situations. In this session, our speaker will discuss these techniques to enhance your interviewing skills to spot the liars from the truth-tellers. These will greatly aid in your own cybercrime investigations.

**Keynote: The Office Of Cybercrime Initiatives**

**Hon. Emmanuel Caparas**, Undersecretary, Department of Justice and Chief, Office of Cybercrime

The recently issued Implementing Rules and Regulations (IRR) for the Cybercrime Prevention Act spells out the specific roles of various government agencies in combatting cybercrimes. The central authority is the Office of Cybercrime housed in the Department of Justice (DOJ). Our keynote speaker, Hon. Emmanuel Caparas, will provide an overview of the DOJ’s efforts and present the plans of the Office of Cybercrime for 2016.

**Cybercrime Law Enforcement Panel**

Philippine National Police & National Bureau of Investigation

This session features the primary law enforcement agencies tasked with investigating cybercrimes and apprehending violators of the Cybercrime Prevention Act. Both the PNP and NBI will discuss past cases and identify the current trends in local and cross-border cases. They will also feature the services they provide to victims and complainants including digital forensics, surveillance, raids, arrest and preparation of initiatory documents for the prosecution of offenders.

**Cybercrime Updates: The IRR of the Cybercrime Prevention Act**

**Atty. JJ Disini, Managing Partner**, Disini & Disini Law Office

After the Supreme Court for the most part, upheld the validity of the Cybercrime Prevention Act, the government issued the Implementing Rules and Regulations. This session will discuss those developments as well as the challenges of prosecuting cybercrime cases.

**Emergency Response to Cybercrime Events**

**Mr. Albert dela Cruz, Director**, Philippine Computer Emergency Response Team

Cybercrime emergency requires interventions in different domains. Many questions arise in the midst of an on-going emergency. What should we do? Should we shut down? Should we disconnect from the Internet? What do we tell our employees to do? How to we minimize damage or prevent further damage? How should we handle this internally and externally? This session will present best practices in the field of emergency response and will aid participants in striking a balance between defending the network and minimizing damage to your infrastructure and reputation.

**Preventing Cybercrimes**
Mr. Henry Aguda, Chief Technology and Information Officer, Amihan Group

Benjamin Franklin famously said “An ounce of prevention is worth a pound of cure.” Recent hacks have certainly demonstrated that. The famous Sony Pictures hack cost the company $35M in IT repairs and untold losses in reputational costs. Sony even paid its employees $8M to settle claims arising from the breach of personal privacy. The US retailer, Target, was the victim of a data breach that resulted in out-of-court settlements to its customers and Visa in the amount of $10M and $67M, respectively. This session aims to provide practical tips to secure your network, identify the weak links in your security chain, and identify interventions that can aid in improving your efforts at avoiding a cybercrime event in your organization.