
Cybercrime & data breach

Experience and innovation across the globe

Advisory Services

Forensic Services

The complexity of cybercrime

Online onslaught. Blurred boundaries. Corrupt insiders. Cyber threats are varied, complex, and always evolving. Preventive and defensive measures may reduce risk, but do not eliminate risk of internal usage policy violations, computer intrusions, data loss, and asset sabotage. Cybercrime is committed by a multitude of offenders with diverse motives: insiders with authorized access behave badly; competitors want an advantage; foreign governments commit economic espionage; terrorist organizations disrupt services; and transnational criminal enterprises steal for profit.

The ability to forensically investigate cybercrime is critical to protecting data, the infrastructures that store and transmit data, and the organizations responsible for those infrastructures and data. Personally identifiable information, payment card information, medical records, intellectual property, trade secrets, etc. can be converted by unsavory forces into financial gain. In the process, the reputations and operations of those victim organizations can be negatively impacted.

The information technology (IT) infrastructures that house data and permit its movement are assets that improve organizational efficiency and effectiveness. Intentional denial of service of these infrastructures can have immediate and detrimental outcomes on revenue and customer confidence. Worse, disruption of the IT infrastructure of organizations deemed as critical infrastructures by the U.S. government can have national security implications. Also, gaining unauthorized control of these infrastructures or the data of any organization can be quite profitable to those with an extortionate mindset.

Therefore, speed is essential when investigating suspected cybercrime. The life span of digital evidence is short. When a cyber breach or data theft is discovered, quick response, forensic preservation of digital evidence, and the application of the right analytical methodologies on the digital evidence are critical to an efficient resolution.

Most organizations do not have the luxury of staffing an in-house cybercrime investigative team, so when a situation does occur, companies that have collaborated with the right cybercrime investigative firm will be better positioned to manage the myriad of potential legal liabilities and reputational issues.

How PwC can help: Forensic Services

PwC has forensic and investigative professionals across the globe ready to respond and assist you in the fight against cybercrime. Our goal is to serve as your forensics, investigative, containment, remediation and compliance resource anytime you have an incident or a concern.

The right firm should have forensic personnel, technology, and laboratories located in strategic geographic locations and leaders who are experienced in cybercrime matters. The right firm should have a pool of talent permitting the deployment of the right personnel for the situation at-hand and be able to augment its cybercrime investigative team up or down based on the depth and breadth of the matter. Further, the right firm would ideally be able to introduce industry-specific specialists to provide advice, business impact analysis and protected data specialists (payment card industry, medical records, student records, etc.) to assist with navigating the regulatory waters of certain protected data types.

For more information, contact:

Dave Burg
(703) 918-1067
david.b.burg@us.pwc.com

Shane Sims
(703) 918-6219
shane.sims@us.pwc.com

Ed Gibson
(703) 918-3550
ed.gibson@us.pwc.com

Kimberly Peretti
(703) 918-1500
Kimberly.k.peretti@us.pwc.com

David Nardoni
(213) 356-6308
david.nardoni@us.pwc.com

Tomas Castrejon
(415) 498-8418
tomas.m.castrejon@us.pwc.com

Forensics and investigative experience. Successful investigations demand professionals with the right skills and experience. PwC's cybercrime investigative teams are comprised of forensic technology specialists, Certified EnCase Examiners, Certified Information Systems Security Professionals, attack & penetration specialists, crisis leaders, former cybercrime prosecutors and attorneys, and former law enforcement agents.

Global reach. Our forensic and investigative professionals, and digital evidence labs, are located in major business centers throughout the world and regularly provide cross-border services to complex global companies. Our professionals are located where you do business and are conversant in local language and culture and regulatory issues.

Digital evidence collection and analysis. Our investigative team will collaborate with your IT department to forensically preserve affected systems and data and acquire pertinent logs from monitoring technology in a manner that is least disruptive to your production environment. If an insider(s) is suspected, our investigative team will collect email, network stored files, and locally stored files on workstations and mobile computing devices including PDA phones used by the suspected insider(s). This evidence will be analyzed by experienced professionals and the analysis can be performed onsite or at one of our digital evidence labs. Our professionals leverage proprietary tools to analyze a myriad of data sets in new and innovative ways. Further, our professionals can manage your eDiscovery needs in response to civil litigation.

Malware analysis. If malicious software is discovered during the investigation that was not detected by in-house technology, professionals in one of our digital evidence labs will analyze the malware to determine its functionality and purpose. This analysis permits our clients to take immediate actions to identify other instances of the malware across the environment and prevent its communication with unauthorized systems and prevent its ability to egress data.

Electronic surveillance. If legally authorized, we can deploy network-based and host-based electronic surveillance technologies and professionals to monitor the actual or suspected cyber-based activity.

As your trusted advisor, PwC will seamlessly integrate with your in-house teams to investigate these risky situations. We continually invest in current technology and facilities to support our client's needs and our investigative capabilities. We also provide ongoing training, continuous improvement and knowledge-sharing programs for our people, so that everywhere we operate you can be certain of a uniform excellence and sound methodologies as well as intelligent, valuable, experience-based advice and quality service.

Improving reactive and proactive measures

PwC works with clients in responding and reacting to cybercrime matters effectively by creating contractual vehicles permitting quick deployment of our global forensic services resources. As a result, our clients are better positioned to investigate, contain, and remediate cybercrime incidents and manage inquiries from law enforcement, regulators and civil suits.

Leveraging cybercrime investigative techniques enables you to improve your security posture and reduce risk in creative and innovative ways. PwC's cybercrime services can be engaged to assess an organization's cyber space for indications of malicious activity that is not being detected by in-house technology and people. Conducted under the privilege of a legal risk assessment, the findings of our proactive cybercrime investigations are protected and can be quickly used to neutralize an in-progress attack or reduce the risk of a successful compromise.

pwc.com/us/cyber

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2011 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.