

---

# Cyber security incident response

## Advisory services Forensic services

Cyber-based risk can be reduced to a minimally acceptable level but not be completely eliminated. Threats to IT infrastructures and the data within it are varied, constantly evolving, can be externally or internally born, and originate from both hostile and trusted sources. However, those organizations prepared to respond swiftly and forensically to a cyber breach incident will be capable of defending themselves from a myriad of critical consequences.

Failure to respond immediately with resources experienced in crisis management, cyber investigative techniques and the appropriate methodologies and technologies can result in significant financial losses and irreparable damage to your company's reputation.

While critically important, forensic investigative experience is generally not a core competency of leading global organizations. Simply put, it is seldom practical for most companies to maintain the requisite forensic investigative resources and technologies necessary to effectively conduct complex cyber investigations.

### How PwC can help

**Forensics and investigative capabilities.** PwC's cyber incident response teams are comprised of forensic technology specialists, Certified EnCase Examiners, Certified Information Systems Security Professionals, attack & penetration professionals, crisis leaders, former law enforcement agents and former cybercrime prosecutors and attorneys.

**Global reach.** Our forensic and IT security professionals are located in major business centers throughout the world and regularly work in global teams to provide cross-border services to complex multinational companies.

**Rapid response.** PwC's professionals are accustomed to responding on short notice to the needs of clients and their complex data environments.

**Forensic technology.** Our forensic team will coordinate with your IT resources to efficiently secure and analyze compromised systems and electronic information. PwC has digital forensic labs located throughout the world where our professionals leverage proprietary tools to analyze a myriad of data sets in new and innovative ways.

**Flexible approach.** Although PwC has defined and proven incident response protocols and guidelines utilized by our teams, we tailor our approach to the specifics of the matter at hand and perform only those services that will provide you with the value and the impact required.

### Calm and reasoned

Working closely with your team, PwC will manage and coordinate the investigation.

We will provide you with a timely and assured understanding of what happened and do so in a manner that will withstand judicial and regulatory scrutiny. The result is a cost-effective, thorough investigation, giving the peace of mind that comes from a trusted forensic advisor.

---

# Cyber security incident response

## For more information, please contact

---

**Dave Burg**

(703) 918 1067

david.b.burg@us.pwc.com

---

**Donald Christian**

(703) 610 7500

donald.b.christian@us.pwc.com

---

**Shane Sims**

(703) 918 6219

shane.sims@us.pwc.com

---

**Everett Vance**

(703) 918 1460

everett.r.vance@us.pwc.com

---

**Roderick Castillo**

(703) 918 3934

r.m.castillo@us.pwc.com

---

**Michael Amadei**

(703) 918 3051

michael.d.amadei@us.pwc.com

---

**Robert McKinney**

(703) 918 1205

robert.m.mckinney@us.pwc.com

---

**Ed Gibson**

(703) 918 3550

ed.gibson@us.pwc.com

---

**Kimberly Peretti**

(703) 918-1500

kimberly.k.peretti@us.pwc.com

---

## Impact

Forensic investigations and systems/data analysis are always complex but especially so under crisis conditions. As your trusted advisor, PwC will work closely with your in-house teams to understand, mitigate, and manage these high risk situations. With more than 300 dedicated professionals in over 30 countries, we understand local legislative and cultural environments.

We invest significantly in developing and maintaining facilities, technology and software. We also invest in ongoing training, continuous improvement and knowledge-sharing programs for our people so that everywhere we operate, you can be comfortable with consistent delivery and sound methodologies.

**Deployment of resources.** Upon notification of a cyber security incident, we will deploy the right people who are armed with the right technology based on the situation at-hand. This team can quickly be scaled and augmented by internal PwC resources to support the dynamic nature and nuances of any given cyber incident.

**Arrival on-scene.** Our investigation team will meet your incident response team to get a current situation report. A plan for investigative status updates and integration into your crisis response communication plan will be developed.

**Forensic collection of systems and data.** Our investigative team will collaborate with your IT department to forensically preserve affected systems and data and to acquire pertinent firewall logs and logs from other monitoring technology in a manner that is least disruptive to your production environment. If an insider(s) is suspected, our investigative team will provide creative solutions to consider.

**Systems and data analysis.** All computers suspected to be compromised and/or used as a tool to conduct the cyber security breach will be analyzed to help identify the who, what, where, when, and how. Known compromised systems storing protected data (PII, PCI), intellectual property, or sensitive propriety data can be further analyzed to present the extent of the actual or potential theft in support of legal and regulatory needs.

**Containment.** Our team will collaborate with your IT department to develop a plan to contain the incident, prevent further damage, and remediate control weaknesses based on the findings of the investigative efforts.

## 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 and 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.