www.pwc.ch/forensic

Cyber Investigations

When an incident occurs the first few hours are crucial

Dealing with today's cyber threat isn't simply a question of reviewing your security systems.

To respond appropriately, you need to have the flexibility to act quickly, gather the facts and assess the true impact of the loss to your organisation.

pwc

As the cyber threat grows so does the need to respond quickly and effectively

"The Internet, with its incredible connective power, has created opportunity on a vast and growing scale... But there is a darker side to cyberspace that arises from our dependence on it"

William Hague,
British Foreign Secretary

"The average cost for the worst incident now ranges between £280,000 and £690,000."

Information Security Breaches Survey (ISBS)

"Cyber Security comes top of the five 'risks to watch' ahead of weapons of mass destruction and resource security"

World Economic Forum Global Risks 2011 Report

Cyber Crime is a growing risk to organisations

No longer limited to targeting customer data and disrupting web sites, cyber criminals can now target any organisation's IT systems for a variety of purposes.

Attacks can be designed to disrupt business continuity, misappropriate sensitive data, and even jeopardise the safety of corporate infrastructure. These incidents can have serious commercial consequences for an organisation.

In today's connected world, all data is at risk from elements across the globe

Threats can come from inside an organisation as easily as from external parties. A recent case involved an attack on a client's customer data in Asia that was perpetrated by a UK employee for fraudulent use in another country. Often the perpetrators will be operating in a different territory to their victims.

In some instances, intellectual property has been sold to competitors or used in counterfeiting; in others, data has been used to defraud the organisation or misappropriate assets.

Furthermore, damage from data breaches and cyber threats often extends beyond the direct loss of data to include loss of revenue, damage to business integrity, decreased competitiveness, regulatory sanctions and ultimately reputational damage.

You need to counter cyber threats and protect your data

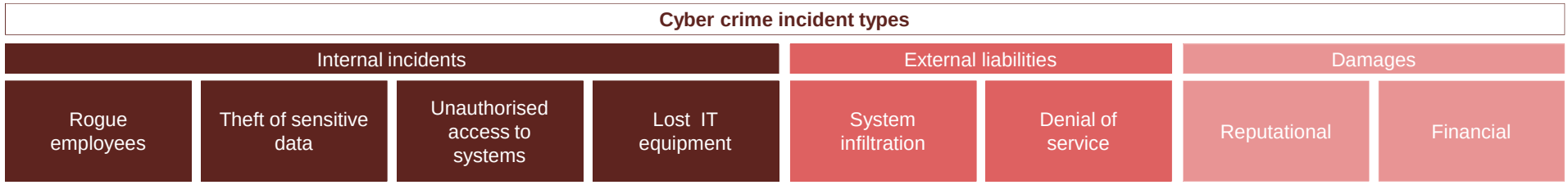
It is vital you have access to the right resources to deal with the growing cyber threat to your organisation. You will need to understand how and who has breached the systems as well as the real impact of the breach on your organisation.

How you respond in the first few days if not hours can have a major impact on the chances of a successful outcome to an investigation. Ideally, you should already have a response plan in place that ensures the right resources can be immediately deployed to protect your organisation and its assets.

Understanding the technology is only one aspect of dealing with cyber crime, you need to have the investigative experience and the global reach to deal with the threat

To get the answers you will need investigators who have the flexibility and forensic mindset to uncover and preserve evidence of what happened, when and why.

They will also need to understand the commercial sensitivities, whilst having the technical knowledge and investigative experience to act quickly and identify the threats to your organisation.



Responding to a cyber incident

You need the right approach to protect your organisation

Often organisations will approach a cyber incident in a reactive manner, reaching for their service provider or information security team to plug the gap in their system. However, they also need to consider the commercial impact and what evidence they need to identify the culprits. Failure to deploy the appropriate resources can limit an organisations ability to respond to an incident and cause irreparable damage to its reputation.

Simply put, it is seldom practical for most companies to maintain the requisite forensic investigative resources and technologies necessary to conduct complex cyber investigations.

However it is important to have access to these resources where an incident occurs. The diagram below is an outline of our investigative approach to a cyber incident.

Crisis Management is a key part of a Cyber Investigation

Forensic investigations and systems/data analysis are always complex but especially so under crisis conditions.

However, while critically important, forensic investigative experience is generally not a core competency of leading global organisations. This is particularly important when there is a requirement that your approach will withstand judicial and regulatory scrutiny.

What we have done for our clients:

- A global bank's secure banking system had been breached, exposing confidential client data. Our forensics team were responsible for identifying, capturing and analysing the electronic documents including emails, transactional databases and network server logs.

  During the forensic analysis, the team were not only able to identify the systems and data that had been compromised; they were also able to provide sufficient information to allow the intruders to be traced. Post incident, we advised on business continuity, providing expert advice and assistance on implementing security measures to prevent a similar occurrence.

- We carried out an investigation into the alleged theft of specialist technical data by a former employee of a blue chip company. Our forensic investigation of email and internet data demonstrated that the individual had transferred company confidential data to a third party. During the subsequent litigation, our primary role was to advise the lawyers on e-disclosure and matters raised by the court and opposing forensic experts on the electronic evidence.

- We assisted a client in the hospitality and leisure industry with an investigation into an attack designed to steal sensitive data from their IT systems. Our client had previously relied on the investigative capabilities of a third party that was providing IT security support. In the course of the project it became evident that the provider, although expert in IT security, had limited forensic capabilities which meant that vital evidence had not been collected. We were called in to capture the data forensically in order to protect the integrity of the evidence and to conduct interviews of key staff members impacted by the attack. We were also able to advise on the capture and analysis of network logs and the permissions on the email systems which helped the client to identify the weaknesses in their systems that led to the attack.

PwC Investigations Approach

Phase 1: Identity and contain	**Phase 2:** Scope and Assess	**Phase 3:** Collection and preserve	**Phase 4:** Analyse and report	**Phase 5:** Remediate
• Forensically examine the affected systems • Forensically collect volatile evidence • Establish Forensic investigation teams and determine covert or overt investigation	• Assess the impact on business activity • Formulate forensic investigation work streams • Assess regulatory or other reporting requirements • Understand the business' culture and policies	• Interview key individuals in line with relevant legislation • Forensically capture electronic evidence • Generate timeline of key events using evidence collected	• Determine and patch any further vulnerabilities • Present findings and recommend next steps • Comply with necessary legal, regulatory or other reporting requirements	• Develop improvements in policy and procedures • Train and educate employees in best practice • Assist with legal and regulatory action as required
Hours to Days	Days to Weeks	Weeks to Months		Continuous

Investigate

Our approach combines professional forensic investigations experience with specialist skills in information security

Gianfranco Mautone

Partner, Leader Forensic Services
Tel: +41 58 792 17 60
Email: gianfranco.mautone@ch.pwc.com

Jürgen Müller

Partner, Leader OneSecurity
Tel: +41 58 792 81 41
Email: juergen.mueller@ch.pwc.com

Thomas Koch

Director, OneSecurity
Tel: +41 58 792 29 54
Email: thomas.koch@ch.pwc.com

Stephan Teiwes

Senior Manager, GRC IT Risks
Tel: +41 58 792 27 96
Email: stephan.teiwes@ch.pwc.com

In order to deal with the cyber threat effectively organisations need to ensure that they are well prepared to survive an incident. Their response to today's breed of cyber crime should reflect the realities of the evolving landscape, therefore it is important to plan ahead and ensure they have the right resources in place both internally and externally to undertake an investigation and deal with the threat

We have the ability to deploy multi-disciplinary teams of forensic investigators, security professionals and crisis management experts. If you would like to find out more about cyber investigations, or our full range of cyber security services, please contact us.

PwC Cyber Security Services

www.pwc.ch/forensic

Design: ML1-2011-08-31-0904-AA