Representative engagements

IT infrastructure assessment
An African supplier of infrastructure services engaged EY to determine if it had a network breach and, if so, the extent of the breach. The company also asked EY to help identify areas for improvement with its network security policies and procedures.

The EY team collected network traffic data on the internal network going to/from non-affiliated sites on the internet, as well as data from 122 key network servers, with a view to disrupting services to the businesses. Analyses on both network and system data revealed:

► Active network intrusion dating back five years
► Misuse by IT personnel
► Network and system configuration errors that exposed critical business information on the internet

Cyber intrusion investigation
A European top-level domain name registrar requested EY’s assistance in investigating an external intrusion. The domain names for major international companies had been hijacked that site visits were directed to inappropriate internet sites.

EY collected and analyzed data to isolate the intrusion mechanism, and also evaluated the network infrastructure to determine whether the intrusion had gone beyond the initial attack vector. The final results showed that the intrusion was indeed limited in scope, which EY’s client was able to demonstrate to its clients and government regulators. Our analyses also revealed that a key internal server had been misconfigured, which led to exposure to external intrusion.

Targeted network intrusion investigation
A major European defense contractor retained EY to investigate a targeted network intrusion. The client had previously engaged one of our competitors to assist with previous network intrusion investigations, but was dissatisfied with its approach and results.

EY advised on the investigation approach and the development of an implementation plan. In addition, we processed over seven billion packets of network data provided by the client, which subsequently revealed:

► Active malware in the network environment
► Connections to external services with clear-text passwords
► Misconfigured routers, firewalls and services
► Possible leakage of intellectual property

EY advised on the investigation approach and the development of an implementation plan. In addition, we processed over seven billion packets of network data provided by the client, which subsequently revealed:

► Active malware in the network environment
► Connections to external services with clear-text passwords
► Possible leakage of intellectual property

Have your computer systems been compromised?
Cybercrime is increasingly going undetected, as organizations face a persistent and sophisticated threat from attackers.

Criminals are targeting commercially sensitive information, intellectual property and critical network infrastructure. These threats may come from attackers both within and outside your organization.

Some of these may seem harmless and others far more damaging and malicious than in their intent. Nevertheless, any intrusion into your computer systems can lead to regulatory fines, operational expense, reputational damage and loss of competitive advantage. No organization wishes for its closely guarded secrets to be traded or leaked out into the open.

Many vendors are creating products to help counter the threat. Companies are deploying sophisticated virus detection tools, intrusion detection systems and data leakage prevention appliances. Despite this armament of technology, high-profile and damaging breaches continue to be publicized in the media.

Cyber threats were once considered an issue for the information technology (IT) department alone. However, increasingly, such threats are being discussed in the boardroom, as the authorities hold companies and their leadership to account for the security of customer and employee data.
A new challenge

Our experience shows that companies understand the need for effective cybersecurity, but are aware that such controls and technologies alone cannot entirely eliminate the threat.

Often, network security appliances are put in place to detect intrusions and monitor data leakage. These are used to fend off widely known threats, but are not in themselves a viable defense against a motivated attacker.

IT managers can quickly find themselves overwhelmed with vast amounts of security log data that is never cross–matched or effectively reviewed and prioritized. There are also very few systems that can look below the surface of an organization’s IT landscape to uncover the forensic tracks that remain obscured to an attacker.

When breaches are discovered, they are often remediated immediately without executing a full investigation into the attack. This can leave other parts of the network compromised and exposed, as the full extent of the breach is never uncovered.

What is clear is that IT and risk personnel need to consider how to protect their IT systems from cybercriminals, but must also consider:

► How to determine whether attackers have slipped past the security defenses
► What can be done if they have

We believe that a proactive forensic approach will help your organization respond to complex incidents that may have breached your security. This will help reduce the amount of time a network is exposed, mitigate the damage or data loss that results and increase the probability of catching the perpetrator.

Our approach

Our cybercrime investigation team is comprised of IT forensic and security professionals working closely with experienced corporate investigators. We are often asked to investigate and respond to network breach incidents, but increasingly we are advising clients to take a more proactive approach.

It is typical to assume that your IT network has not been breached and to focus your efforts on keeping out attackers. A more effective approach is to take a different starting position.

Our teams will assume that you have already been targeted and will focus on investigating your IT estate for any evidence of data theft or intrusion.

Our service

Our team has developed an approach to sampling networks for indicators that a breach may have occurred. This is in contrast to a traditional IT audit or a vulnerability test, which focus on potential weaknesses to common, well–publicized attacks. Our cybercrime diagnostic focuses on those targeted attacks that are designed to slip past your defenses.

Initially, we will review your network architecture and take samples of forensic artifacts where we know breach indicators can reside. Typically, such artifacts include a sample of network traffic, server and appliance logs and a selection of forensic artifacts from key computer systems or servers.

This data capture process is tailored to reduce the support required by your busy IT teams and is not likely to have a significant impact on the performance of your infrastructure.

Following collection, we use a variety of automated forensic tests, data mining technologies and the experience of our staff to highlight indicators of potentially suspicious activity.

What can we find?

The initial analysis will allow us to identify further workstreams for additional investigation. For example, these indicators can include:

► Evidence of the use of remote access software from unauthorized sources
► Indicators of the presence of active malware
► Persistent connections to other countries or unauthorized entities
► “Back channel” data flow into/out of your organization
► Indicators of data harvesting by employees or leavers
► Unauthorized system and data access

In addition to these indicators, we often uncover other findings that relate to your IT security or information governance regime, including:

► Limitations of existing security policies
► The storage of confidential data in unprotected areas (webmail, cloud storage, etc.)
► Inappropriate use of IT resources
► Misconfigured network devices
► Installation of unauthorized software or hardware

Our analysis is data–driven. Our approach scrutinizes any indicators that are suspicious, rather than being restricted to a narrow set of rules.

Investigation and remediation

The output of our analysis will likely or probably be the identification of a number of issues that can be passed directly to an IT remediation or investigation team. These issues should be prioritized according to your objectives and the perceived severity of the threat. For example, you may allocate internal IT resources to the mapping and eradication of a seemingly innocuous botnet. Similarly, you may instruct an in–house forensic team to investigate indicators of a possible internal data theft.

Alternatively, you may feel that a full investigation of an external compromise of your document repository by our cybercrime team is warranted. We can help you to manage this complex web of multiple investigation and remediation work streams.

As experienced forensic analysts, we can also help you throughout the life of any subsequent dispute or investigation. We can provide litigation support to your legal team and can serve as expert witnesses, where required.

Ongoing support

A cybercrime diagnostic is similar to a vulnerability assessment, insofar as it should be undertaken at regular intervals. We can help your organization take this process in–house and would be happy to advise you on processes and methodologies as we get to learn more about your IT landscape.

Through a close, ongoing relationship, we can also enhance your ability to respond to incidents when they occur and protect your organization.