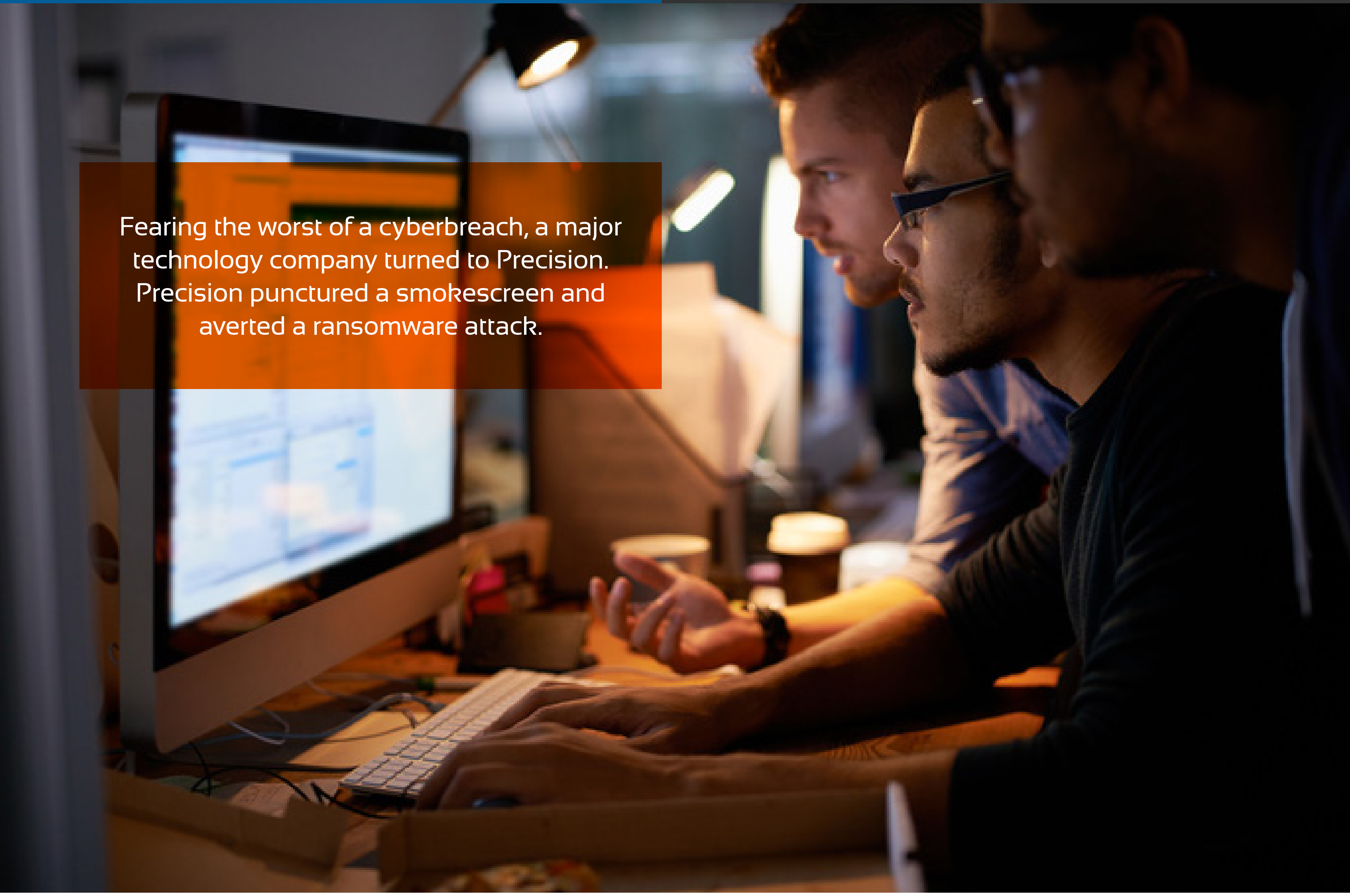
CLIENT SUCCESS STORY

Cyberbreach Forensic Analysis



Fearing the worst of a cyberbreach, a major technology company turned to Precision. Precision punctured a smokescreen and averted a ransomware attack.

In a cyberbreach crisis, Precision gets to the root cause and thwarts further attack.

EXECUTIVE SUMMARY

A major U.S. technology company with a highly capable network and security operation had detected a security breach in one of its networks with the installation of unauthorized software. At first, they suspected a malicious insider, but as the attack expanded, they feared a larger threat.

Precision's experienced forensics and security experts determined the cause of the security breach and prevented its spread to other networks. Precision helped the client triage the incident and limit its impact, avoiding a costly and potentially catastrophic outcome.

The Challenge

The Network Operations Center (NOC) of a major U.S. technology company detected unusually high CPU use in one of the 1000+ networks and systems it monitors. NOC personnel alerted the company's Security Operations Center (SOC), which immediately deployed an incident response team to investigate.

The team quickly discovered Bitcoin "mining" software running on the affected network. Digital currency miners often try to co-opt the resources of large and powerful computer networks, so the company assumed it was an inside job – an employee using company hardware to run unauthorized Bitcoin software.

Two days later, the mining software spread across multiple networks within the organization. Fearing that the threat was larger and more sophisticated than initially believed, the company engaged Precision Discovery's forensic and security experts to ascertain the root cause of the incident and assess the exposure to the company and its data.

The Precision Solution

Precision's team performed a comprehensive forensic analysis, using a suite of forensics strategies and tools to determine the cause of the security breach and prevent its spread to other networks. Precision started by preserving and analyzing all data and system information as well as live network traffic from one of the affected networks, including:

- **Network artifact recovery** and **analysis**
- In depth Internet **Traffic** and **Packet Capture** (PCAP) analysis
- **System** and **Security Event Log analysis**
- **Library** (e.g.DLL) and **RAM analysis**
- **Forensic examination** of traces of how/when/where the mining software appeared and what it affected.

Precision's analysis revealed something unexpected: suspicious connections to and from various foreign nations into the company's network. The hackers exploited an open, unsecured port in the company's domain controller to perform brute force attacks on administrator accounts. Once logged in as an administrator, they could freely access the company's internal networks.

The Bitcoin mining software was merely a diversion. As Precision's team continued to investigate, it found that the hackers had installed ransomware to prevent the company from accessing its data until a ransom was paid. However, once Precision identified the specific type of ransomware, the security team used decryption tools to undo the damage without paying the ransom. Precision also determined that while the hackers had collected confidential internal data, no personally identifiable information (PII) about the company's customers was compromised – a huge sigh of relief for the client.

The Results

In this case, Precision's forensic analysis helped the client triage the cyberbreach and limit its impact. Precision helped the client understand their exposure and provided security recommendations to prevent further breaches.

Through the diverse expertise of the Precision team, we help clients diagnose issues and deliver effective solutions in a wide variety of circumstances.

PrecisionDiscovery

25 West 45TH Street
New York, New York 10036

877-897-4545

info@precisiondiscovery.com

www.precisiondiscovery.com