



## REACT CASE STUDY

### CLIENT GOALS

- Isolate and eradicate insidious information exposure quickly
- Obtain recommended action plan for preventing future breaches

### SITUATION OVERVIEW

A leading global full-service print solution provider suffered a massive security breach requiring urgent information recovery, restoration of secure databases, and resumption of business operations.

Server downtime due to the exposure cost the company an estimated \$200,000 per hour in addition to potentially jeopardizing customer loyalty and pending contracts if news of the breach were to become public.

As a dominant player in their competitive industry, the provider was a prime target for security breaches.

### ECLIPSECURITY SOLUTION

Eclipsesecurity Ohio office immediately assembled and deployed one of its on-call incident response teams to work around-the-clock to quickly and adeptly execute a multi-phase reactive operation.

#### Phase I: Assess source

Diagnosed source as combination of email-borne virus and covert Trojan. Thorough and swift investigation utilized digital intrusion detection solutions, including both automated security scanning tools and manual Eclipsesecurity-proprietary proven processes.

#### Phase II: Identify scope

Isolated and contained exposure from further short-term propagation while virus and Trojan destruction in progress. Required closing impacted ports and protocols as well as decommissioning much of client's network.

#### Phase III: Eradicate exposure

Eliminated source of breach and continued exposure. Required rebuilding impacted servers and workstations, performing NetBIOS and OS/platform cleansing activities, conducting triages, and developing and maintaining procedures to preserve potentially jeopardized data.



#### **Phase IV: Restore secure business functions**

Performed rapid test quality checks and penetration inspections prior to resuming business operations.

#### **Phase V: Recommend action plan to insulate the company from future exposure**

Worked with management to align future growth initiatives with security imperatives.

### **RESULTS**

Eclipsecurity was retained to establish a comprehensive security incident response plan, including digital forensics, across the client's global operations.

- Information exposure was isolated, source eradicated, and data recovered and secured with minimal interrupted business operations.
- With Eclipsecurity as a continuing resource, the print solution provider has experienced no further breaches impacting business continuity, an impressive metric in this competitive industry.