SecurityScorecard

CASE STUDY

SecurityScorecard Helps Auction Company Prepare for Information Security Incidents

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

THE CHALLENGE

This world-renowned auction company has been one of the leading businesses in the art industry since 1766. Known for its live and online auctions, the company has a physical presence in 46 countries.

For 250 years, this company has been a trusted steward for great works of art, and is paving the way for digital innovation in the industry by pioneering new technologies, bidding and viewing experiences, and buy-now channels.

This company understands the importance of maintaining business continuity in the event of a cybersecurity incident. And to ensure this could be achieved, it set out to proactively test its preparedness.

GENERAL INFO

COMPANY

Auction

INDUSTRY

Arts and Auction

LEVEL 1 MSSP ABILITIES USED

Business Continuity Plan

Isolated Backup Storage

Ransomware Awareness

Ransomware Response Plan

USE CASES

Business Continuity and Ransomware Readiness

WHY SECURITYSCORECARD

Provides managed services required to maintain business continuity and ransomware readiness

THE SOLUTION

SecurityScorecard conducted simulated security incident exercises alongside the company's stakeholders to assess its preparedness to respond to security incidents. The exercise covered the identification, containment, eradication, and recovery stages of incident response.

The scenario revolved around the potential compromise of the company's systems by a threat actor who deployed ransomware and exfiltrated data. The exercise itself focused on how the company would react and respond to this threat, and the decision of whether it would pay a ransom for the return or deletion of its data.

With SecurityScorecard's help, the company was able to test its Incident Response Plan (IRP). Participants from the company competently and effectively implemented the plan and demonstrated a good understanding and technical knowledge of their environment and the regulatory regime in which it operates. Although the exercise was a success, SecurityScorecard found a few key areas to improve.

THE RESULTS

The first area for improvement focused on determining the systems and services needed for auctions and under what circumstances the company would cancel an auction. For critical, revenue-generating operations, including auctions, SecurityScorecard recommended the company do the following:

A. Articulate the essential technology services and systems that are required, and document the contingencies and alternatives if these services and systems are unavailable.

B. Determine who would make the call on the cancellation of an auction, and under what circumstances an auction could be canceled.

C. Host auction-specific tabletop exercises to determine the steps needed for the company to hold auctions during incidents and events.

During the exercises, SecurityScorecard found that the regular communications channels the company uses could be compromised by threat actors. It was recommended that the company explore an out-of-band communication process to communicate with incident response personnel via private email accounts and mobile phones in the event of a serious outage or incident. Additionally, the company was advised this process should be actively maintained with up-to-date details and regularly tested.

SecurityScorecard helped the organization strengthen its security awareness program by proactively communicating the following measures users should take during an incident:

A. Refrain from sharing, posting, or commenting publicly during such incidents.

B. Disconnect laptops from networks if they are suspected of being infected.

C. Explore an out-of-band communication option to communicate with ALL users, via private email accounts or phones.

In addition to strengthening internal communication during an incident, SecurityScorecard helped the company provide clarity around when to engage law enforcement the U.S. and all major markets. Key points of clarification were:

A. Decision and timing of engaging with law enforcement.

B. Who would engage with law enforcement?

C. How law enforcement communications would be aligned with wider stakeholder engagement and communications.

The incident response exercises revealed that the company did not have documentation of its most sensitive data, where it is located, and who owns it. To bolster ransomware awareness, SecurityScorecard helped the company ensure that information owners are in place and that users apply data classification labels to files and folders, denoting the sensitivity of the information they contain. This is critical to accurately determine the extent of data exfiltrated and its material impact.

In a real incident, it can be difficult to accurately define when the incident started, and when a data breach was detected. SecurityScorecard helped the company clarify the difference between an incident and a data breach, as

THE RESULTS

defined by its Information Security Response Plan and Data Breach Protocol. This is critical for its regulatory reporting requirements. An incident should be declared as a data breach when:

A. The incident response team has reasonably exhausted all other possibilities – for example, it has determined that the outage has not been caused by failed patches, updates, upgrades, or outages of a third-party system.

B. Clear evidence is found that a threat actor has been within the company's environment – for example, a ransom note is found, or a sensitive data is found on the Internet or dark web.

The company approached the decision of whether to pay the ransom as a cost-benefit analysis, but participants did not quantify the cost of the incident. SecurityScorecard helped establish a cost-benefit analysis process for determining whether to pay a ransom, based on:

A. **Productivity** – Have auctions been canceled? Are future auctions likely to go ahead? What is the expected revenue that these auctions will bring in?

B. **Cost of responding to the incident, recovering data** – What is the cost of third-party cybersecurity firms, outside counsel, specialist communications, and PR support?

C. **Cost of replacement systems** – Will the company be able to recover existing IT assets, or would it need to buy new ones?

D. **Fines, judgements, compensation** – Can these fines be estimated?

E. **Reputation** – Can the company estimate the number of customers who might move to rival organizations?

SecurityScorecard was impressed by the competence and effectiveness of the company's team. Interesting learning points emerged from the exercise that helped to challenge the participants and identify areas to improve the company's Incident Response Plan.

ABOUT SECURITYSCORECARD

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve, and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
New York, NY 10017
1.800.682.1707

SecurityScorecard