SecurityScorecard

CASE STUDY

SecurityScorecard Helps Scientific and Educational Non-Profit 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 worldwide non-profit organization has been promoting environmental and historical conservation since 1888. It supports science, exploration, education, and storytelling to inspire change and protect our world.

With millions of people around the globe participating in, and benefiting from its programs, the organization needed to be prepared to maintain continuity in the event of an information security incident. To ensure this could be achieved, it set out to test how well its Incident Response Plan (IRP) would perform if it was activated during a cybersecurity event.

GENERAL INFO

COMPANY
Non-Profit

INDUSTRY
Science and Education

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 executive information security incident exercises with the main objective to assess the organization's preparedness. The first of these exercises covered ransomware, and the identification, containment, eradication, and recovery stages of incident response.

The scenario revolved around the compromise of the organization's systems by a threat actor who deployed ransomware and exfiltrated data. The exercise itself focused on how the organization 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 organization was able to test its IRP. Although participants from the organization competently and effectively implemented the plan and demonstrated a good understanding and technical knowledge of their environment, SecurityScorecard found key areas for improving the plan itself.

THE **RESULTS**

During the exercises, SecurityScorecard found that participants were decisive in treating three or more devices encountering the same issues as a potential cybersecurity incident, but this trigger or threshold is not reflected in the IRP.

SecurityScorecard recommended revising the IRP d to ensure it lays out specific triggers for its activation. Specifically, this should specify when senior leaders are informed of a potential incident, what information is provided, and how this information will be conveyed.

Additionally, SecurityScorecard recommended the organization should carefully consider the timing of communication with the threat actor. The IRP should outline who will be consulted and engaged in the decision to open communications with the threat actor in the case of a ransomware incident.

SecurityScorecard helped the organization strengthen its security awareness program by including measures that users would be expected to take in the event of an incident. Examples of these measures include:

A. Refraining from sharing, posting any material, or commenting publicly during such incidents.

B. Steps to disconnect their laptops from networks if suspected of being infected.

C. How information will be communicated in the event of a significant outage or incident, including how and when the organization will communicate to a user's private email account.

The incident response exercises revealed the organization did not have documentation of its most sensitive data, where it is located, and who owns it. To bolster ransomware awareness, SecurityScorecard advised completing a revision of the organization's data classification policy to ensure users apply data classification labels to files and folders, denoting the sensitivity of the information they contain.

For a long term solution to protecting data with isolated backup storage, SecurityScorecard suggested migrating data to Google Workspace, which has enhanced data loss prevention policies that help prevent threat actors from exfiltrating data. The security and IT team could then layer on more granular access controls on top of Google Workspace, as needed.

The organization had a mature understanding of how a ransomware incident could impact operations and incur costs, however, it did not have a documented process to quantify the cost of an incident. SecurityScorecard helped to amend its business continuity plan to establish a cost-benefit analysis process for determining whether to pay a ransom. This analysis is based on whether business continuity arrangements could manage and mitigate the costs associated with an incident.

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