Mitigate security threats with IBM Resilient Incident Response Platform for healthcare

Overview

Cyber resilience—the ability to manage, mitigate, and move on from cyberattacks—is a critical goal for the healthcare industry. That's because healthcare is one of the most targeted[1] industries, and hardest hit by cyber threats. Ransomware, in particular, has increased substantially.[2]

The latest research shows:

- The industry faces more cyberattacks than any other industry, including other highly targeted industries such as financial services and government.[3]
- The cost of a data breach for healthcare organizations is USD 355 per record lost, a staggering 125 percent higher than the average organization.[4]
- More than half of US hospitals have been hit by ransomware attacks.[5]

Faced with the challenges of security threats and privacy regulations, healthcare organization security teams are compelled to improve their ability to respond to attacks.

Benefits

IBM Resilient Incident Response Platform® (IRP) orchestrates and automates the entire response process, creating a single hub to connect and manage all your security solutions. By aligning and coordinating your people, process, and technology, Resilient IRP enables faster, more intelligent incident response.

Additionally, Resilient IRP includes the industry's first Dynamic Playbook for ransomware. It prescribes specific, best-practice-based playbooks that help healthcare organizations investigate, assess, and resolve a ransomware attack. And it evolves in real-time as incident information is uncovered to ensure the response is fast and complete.

To help healthcare organizations better mitigate and respond to cyberattacks, IBM Resilient IRP provides three modules: security, privacy, and action. This allows organizations to orchestrate and automate incident response processes and to properly respond to incidents at every stage.

- **Security module:**
  By arming incident response teams with incident response (IR) playbooks, intelligence, and deep-data analytics, the security module helps healthcare organizations ensure their response processes are agile and intelligent.

- **Action module:**
  The action module orchestrates incident response by connecting response procedures to related, integrated cyber security systems. This creates a central hub for IR management, and enables enrichment and remediation actions to drive a rapid and effective response.

- **Privacy module:**
  The privacy module gives healthcare privacy professionals the industry's only instant, highly customizable platform for breach preparation, assessment, and management. This helps ensure fast, efficient and accurate compliance efforts for HIPAA, HITECH, and HITRUST.

Case study: National healthcare provider

A multi-state healthcare provider employed nurses and therapists who traveled as part of their job, and were required to allow physicians with access to patient records. This increased cyber security and privacy challenges. To protect its security, the provider needed a system that would identify federal and state industry regulations that came into play in the event of a breach.

IBM Resilient IRP includes Dynamic Playbooks that outlined the best practices for responding to virtually all incident types. Dynamic Playbooks adapt in real time as information about an incident is uncovered, and eliminate the complexity of HIPAA, HITRUST, and HITECH compliance by providing real-time guidance on data breach notification fulfillment.

The healthcare provider deployed IBM Resilient IRP to tap into a dynamic breach notification knowledgebase and orchestrate effective responses. They were thus able to protect sensitive information while lowering compliance costs.

"If you're going to invest in one thing this year, it should be incident response."

— Gartner

"IRPs like Resilient…[are] a gift that keeps on giving"

— Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group

About IBM Resilient

The mission of IBM Security is to help organizations thrive in the face of any cyberattack or business crisis. The Resilient Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. Many Fortune 500 companies, and hundreds of partners globally depend upon IBM for Resilient best-in-class security solutions.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2018

1 Experian Fourth Annual Data Breach Industry Forecast

2 IDC FutureScape: Worldwide Healthcare IT 2017 Predictions

3 IBM X-Force Cyber Security Intelligence Index

4 The Ponemon Institute, "2016 Cost of Data Breach Study"

5 Healthcare IT News and HIMSS Analytics Quick HIT Survey: Ransomware

Please Recycle

22013622USEN-00