Building a

Cybersecurity Incident Response Plan

ARISTA
Edge Threat Management

CONTENTS

INTRODUCTION

A cybersecurity incident response plan covers what to do and identifies who is responsible for doing it when there is a cyberattack, such as:

- A data breach caused by a phishing or hacking incident
- Loss of access to data caused by a ransomware incident
- Release of data through a supply chain attack
- A breach due to insider threats

Anyone who has consumer or organizational data on a company network, whether on-premise or in the cloud (and this means basically any organization) needs a cybersecurity incident response plan.

Creating a plan, updating it regularly, and revisiting it regularly with new hires and in refresher sessions with your entire staff can help you maintain business continuity and minimize reputational damage in case of a cybersecurity incident.

WHY

you need a plan

Cybersecurity incidents can severely damage your revenues and reputation. Just one breach can cripple an organization due to the cost of data losses, customer churn, and erosion of public trust.

1. Cyberattacks are on the rise and so are their costs, with the average financial damage from a data breach rising 10% from 2020 to stand currently at **4.24 million**[1].

2. Having a robust cybersecurity incident recovery plan can reduce these costs. The average breach takes **287 days to contain,** and among companies with more than 50% of their workforce doing tasks remotely, that time period stretches to **316 days.**

3. Reducing the time to full containment after a data breach to **under 200 days** can drop the costs associated with the reach by as much as 30%, but this can only be accomplished with a **strong cybersecurity incident response plan.**

[1] https://securityintelligence.com/posts/whats-new-2021-cost-of-a-data-breach-report/

WHEN

you should make a plan

The swift and necessary adoption of the cloud, the digitization by nearly all industries and the exodus of the workforce from the office to their homes during the pandemic created new vulnerabilities. The new future of work is hybrid, and these challenges will remain in force.

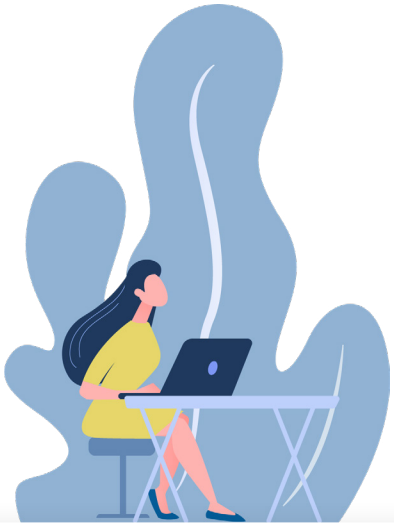
Nearly two-thirds of the CISOs and CIOs expect a jump in reportable ransomware and software supply chain incidents in the second half of 2021[2]. Of those who had experienced an incident in the last 15 months, only 55% or fewer of victims said they were “well prepared” to address the breaches.

Waiting to formulate a plan until after there has been a cyber incident is like shutting the barn door in the wake of escaping horses. The cost of creating an incident response plan and training personnel is a fraction of what a company can lose from a single breach, which is why now is the best time to create a plan.

[2] https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/2021-digital-trust-insights/cyber-threat-landscape.html

WHAT

you need to know to create an effective plan



IDENTIFYING POTENTIAL CYBERTHREAT SOURCES

Who wants company or consumer data? It could be competitors seeking to commit corporate espionage, or hackers looking for data they can use to commit fraud or identity theft or hold for ransom.

IDENTIFYING TARGETS IN YOUR ORGANIZATION

What sort of data is available? Financial data such as payment sources (credit cards or banking information) and personal identifying information (PII) are the most common targets for cyberattacks.

IDENTIFYING WEAKNESSES IN YOUR DEFENSES

A large work-at-home employee base can be a significant risk factor, as multiple devices and logins may be used and endpoint protection can be thin. Using multiple vendors or IoT devices can also create vulnerabilities.

IDENTIFYING WAYS TO STRENGTHEN DEFENSES

Employee education, increased network security, and a zero-trust approach can help prevent cybersecurity incidents from happening. While nothing is 100% foolproof, a layered approach provides the most security.

WHO

is responsible for the plan

Without accountability, a plan is useless. Start from the top, and determine who is responsible for creating your organization's cybersecurity incident response plan. This may be a single person, a team or a third party.

The same process needs to go into deciding who is responsible for updating the plan at regular intervals to ensure all information is correct.

Leaders to spearhead plan execution must be appointed. A clear hierarchy needs to be created, back-ups appointed in case a key person is unavailable, and tasks assigned to specific personnel depending on their skill sets.

Everyone in the organization should be trained on the plan, which necessitates someone being appointed to oversee training sessions and testing of the plan on a regular basis.

HOW

to create your plan checklist

A cybersecurity incident response plan needs to have six components:

Detection & analysis

The first step is implementing warning systems that alert when a breach or attempted breach has occurred.

Immediate response

The second step should be an immediate and robust response, to close the breach and prevent further infiltration.

Containment

The third step is containing the breach, meaning preventing further data loss and attempting to block data accessed from being shared.

Eradication

The fourth step is closing the vulnerability and eradicating the reason the breach was able to be successful.

Recovery

The fifth step is ensuring business continuity or resumption of operations, and setting actions in motion to remediate reputational damage.

Reporting

The sixth and final step includes examining the circumstances surrounding the breach to learn from it and reviewing the response to find ways to improve on the plan.

WHERE

to turn for help

Arista provides a suite of solutions and apps designed to help you improve security and respond swiftly in the face of an incident.

After you've assessed your security risks, you can build your cybersecurity incident response plan that utilizes Arista's Edge Threat Management:

NG FIREWALL

A Comprehensive Network Security Platform

ETM DASHBOARD

A Cloud-Based Centralized Management Platform

MICRO EDGE

A Lightweight Network-Edge Device for Branch Office Connectivity

Get Arista on your team!

Book your free demo now, or contact us today for a free consultation.

ARISTA

Edge Threat Management

edge.arista.com

Arista Networks, Inc.
Santa Clara—Corporate Headquarters
5453 Great America Parkway
Santa Clara, CA 95054

Phone: +1-866-233-2296
Email: edge.sales@arista.com