



The AHEAD Security Event Readiness Checklist

Distilling 10,000 pages
of NIST Framework into
15 key points

Proactive Measures

1

- ☐ Have a documented vulnerability and change management patch program.

2

- ☐ Run ransomware simulations. Focus on threats to endpoints due to the level of risk.

3

- ☐ Have a business impact analysis and asset management program ready. Know where critical assets and servers are and where they interact in the environment.

“ If you don't know what your critical business processes are in the supporting infrastructure, you don't know where to start on a recovery, right?



Wally Guzik

4

- ☐ Know, document and test security incident response procedures, and ensure stakeholder engagement and alignment across the business.

“ Make sure the plan involves the other parties besides IT. Legal is going to need to be involved, PR is going to need to be involved. All the departments that you don't think of initially need to get looped into those conversations.



Tyler Hopperton

5

- ☐ Implement Multi-Factor Authentication (MFA) and privileged account management.

“ The insurance companies will look for MFA.



Christopher Whidden

6

- ☐ Prepare an immutable, isolated copy of your data and your recovery plan, including business critical disaster recovery and tabletop exercises.

“ When was the last time you actually recovered your backups and validated that they were usable? That happens all the time — people recover, but the backup hardware is 1/10th the capacity of what they're trying to recover, and there's not enough room to restore all the files.



Christopher Whidden

7

- ☐ There's no great time for an incident, but have an incident response retainer in place before there's a worst time.

“ There's definitely golden hours for attackers, like late on a Friday before a long weekend. Trying to find an IR partner for boots on the ground on Labor Day weekend — you might as well hold for the winning lotto numbers to get somebody to show up.



Christopher Whidden

8

- ☐ Get cyber event insurance and fully understand what is covered.

“ If you don't have your ducks in a row, you're not getting coverage, or you're gonna get a denied a claim.



Wally Guzik

9

- ☐ The organizations that recover quickest secure the right level of business sponsorship from your executive team.

“ The highest level of senior management should be engaged and involved so that there's some ownership at the highest level, so everything's followed through.



Christopher Whidden

Reactive Measures

- 10 ☐ Your recovery plan is your north star. Routinely check that there are resources and backup hardware in place to execute the plan if needed.

“ This is a very much the Mike Tyson quote of ‘everyone has a plan till you get punched in the mouth.’ You’re waking up with getting punched in the mouth. So you’re not gonna be thinking straight. You need to have this all documented and tested.

 Tyler Hopperton

- 11 ☐ It’s difficult to do analysis after the fact. Ensure access to logs and the ability to search them quickly to identify the impact via telemetry data.

For fast threat identification, the AHEAD SOC utilizes machine learning so that analysts can see the sequence of events leading up to and following a security incident in seconds, painting a clear picture of an attacker’s movements.

- 12 ☐ Have the ability to keep log data protected from attackers.

“ Have good log aggregation and ensure that those logs are safe because attackers will go at the logs. So having multiple sources of telemetry and ensuring that the data is still intact and hasn’t been compromised either is huge.

 Christopher Whidden

- 13 ☐ Monitor your environment and develop a process to evaluate and act on log anomalies.

“ Collecting all the logs is good, but technology by itself is not controlled. You need a process with people to examine the logs and find anomalies or whatever signals we’ve collected and then investigate them. Just like just having a firewall isn’t good enough — you have to be managing it, monitoring it, seeing what it’s blocking, what it’s allowing vs. responding to alerts and events.

 Christopher Whidden

- 14 ☐ Identify who owns the lead response and put it in the plan.

- 15 ☐ Communicate recovery execution, progress, and impact to the business and the board.