AGIO

AGIO INCIDENT RESPONSE MANAGEMENT

The world of cybersecurity has evolved to the point where creating and maintaining a robust security posture is only the first step. The second step is about detection, and the third deals with response. Traditionally, cybersecurity investments have been directed at prevention, but as we become more sophisticated, and the market understands there is no bulletproof prevention method, we're seeing a shift toward the second and third phases: detection and response. Specifically, 68% of companies plan to enhance incident response capabilities in the next 12 months, and Gartner estimates that by 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches—an increase from the less than 30% in 2016.

The ways we protect ourselves are changing, which begs the question, are you changing too?

THE PROGRAM

Agio Incident Response Management is a planned program designed for the unplanned. Over the course of 12 months we onboard, organize, prepare, and continually test your organization's ability to respond when a breach happens. We get—and keep you—battle-ready so when an attack happens, we mobilize immediately and effectively, neutralizing the threat and containing your exposure.

Here's what the program includes:

- Onboarding
  - Environment Discovery
  - Data Mapping
  - Incident Response Plan Development & Review
    - Incident Response Policy
    - Data Classification Policy

        - Incident Response Procedure
        - Incident Response Communication–Chain-of-Command Procedure
    - Tactical/Operational Incident Response Tabletop Exercise
- Monthly Incident Response Readiness Review
- Quarterly Status Review (monthly for first three months after going live)
    - Intelligence Briefings
    - Cybersecurity Events & Incidents Statistics Review
- Annual Executive IR Tabletop Exercise
- Incident Response Annual Review & Report
- Red Team Security Assessment (annually, if applicable)

When a breach actually happens:

- We respond within 15 minutes of discovery.
- We send updates every 2 hours and hold conference calls every 4 hours, for critical incidents.
- We work the incident until it's contained and eradication and remediation plans have been defined.
- We send a full incident report, including recommendations, within 2 weeks of an incident being resolved.

PRACTICE MAKES PERFECT

It's about practicing chaos. You'll never be able to predict the specific type of breach your firm will ultimately fall victim to, but you can predict how you respond. And that response comprises the people you have in place, the processes you've implemented, and the technology that supports it all. How do these three facets interact with one another when tragedy strikes? Where are the loopholes, the gaps, and the ambiguity within your plan? These are the details that, when left undiscovered, unremediated, and unrehearsed, create chaos on top of chaos for organizations.

We're here to fix that. By proactively learning your environment, mapping what data lives where, reviewing your policies with a critical eye, and then practicing chaos, we improve your reaction to a breach. Your response goes from languid, haphazard, and insufficient to immediate, efficient, and—most importantly—effective.

THE INCENTIVE

It's tempting to sit back and hope that a breach won't happen. Or maybe when it does, that it's not that bad. But when your company's operations, reputation, and even your career are on the line, hope isn't a strategy. Because even if the initial breach doesn't bring down your environment, the longer the malicious activity goes undetected and unaddressed, the worse it gets. What may have started as a cybersecurity event, can quickly escalate to an incident and a full-blown breach.

Time is Money

Then there's the financials. Bringing in an Incident Response team only after a breach guarantees one thing; you're going to pay. Why? Because the firm you bring in, even if they're the best, doesn't know your environment.

They don't know where your data lives; they don't know how you collect and store that data (for analysis); they don't know your policies; and they don't know who's involved in your Incident Response Plan. They're flying blind, and it's going to take them time to get up to speed. That's time you're paying for, and even more importantly, that's time in which the breach is getting worse.

By proactively investing in an Incident Response Management service, you drastically reduce your time to resolution, which means less money out the door, less exposure, and ultimately less damage. And you look good because you prepared for the inevitable. You took chaos, mapped it out, prepared for it, and even amortized it (i.e the cost).
Don't you look smart.

WHY AGIO?

#OneAgio

When you select Agio, you're investing in a relationship with everyone who's a part of this firm. Our teams operate in a symbiotic relationship, based on deposits and withdrawals, that creates a vehicle for delivering more than just service. We deliver an experience that reaffirms to our clients we've got them covered. From clean, concise implementations; to consistent support backed by automation and tools that work the way they're supposed to; to value-add reporting; to accurate, timely invoicing; and content on the latest IT and cybersecurity trends, we bring the full breadth and depth of our talent to bear. We deliver #OneAgio.