



AN INTERVIEW WITH ANDY LUNSFORD,
CO-FOUNDER AND CHIEF EXECUTIVE OFFICER,
BREACHRX

AUTOMATE INCIDENT RESPONSE AND READINESS WITH BREACHRX

In today's fast-evolving business landscape, companies not only need to stay on top of responding to the latest cyberthreats, but also have to deal with an ever-increasing pile-on of regulatory and contractual red tape with ever-decreasing response times. Making things worse, incident response and compliance are still often done manually. This is where BreachRx steps in with their automated, dynamic response plans that are custom made for each incident and each's organization's specific needs. We enjoyed discussing their solution at length, and how it helps streamline the incident response process.

TAG CYBER: How does the BreachRx platform help streamline the chaos of incident response and management?

BREACHRX: We founded BreachRx to help companies take back control of incident response. Incidents lead to chaos at most companies, given the complex set of processes that are typically underplanned and ineffectively practiced. Most organizations take a "wait and see" approach, relying on a static paper incident response policy and plan that might be updated or reviewed once a year, and often isn't even opened when incidents actually occur. And while they might have a handle on the technical security processes, most wave their hands at the other, more expensive aspects of incident response. Many leaders we talk to are surprised to learn that only about 30% of the cost of an average-sized incident is the security response. When the inevitable occurs, the key to a successful outcome is readiness. That's where the BreachRx platform comes in—it guides organizations by proactively preparing them for what we call integrated incident response, meaning a repeatable response that includes all aspects, teams, and stakeholders needed to effectively respond to incidents. We replace the legacy plan with intelligent automation by generating tailored response plans that are specific to that organization. The details of each incident are broken down by task and organized by phase, with deadlines. As an incident evolves, the platform adjusts the work required dynamically, bringing in new tasks as necessary and eliminating tasks that are no longer relevant. Our platform gives teams a safe haven to

Many leaders we talk to are surprised to learn that only about 30% of the cost of an average-sized incident is the security response.



operate and collaborate, while protecting legal privilege. We generate audit logs and incident reports automatically based on the actions a company has taken, so teams aren't digging around post-incident trying to figure out what they did.

TAG CYBER: How are increasingly complex cybersecurity and privacy regulations, data breach directives, and compliance requirements affecting cybersecurity, and what can a company do to stay on top of things?

BREACHRX: There are now over 180 regulations in over 120 countries related to cybersecurity and data protection, with more coming at a fast rate. Requirements can be onerous. Besides short deadlines of three-to-four days for regulatory notification, we're seeing potential penalties reach up to 10% of an organization's global revenue. The "best practice" for teams is throwing people at the problem, as well as using spreadsheets, documents, calls, and manual reviews, which clearly don't scale to meet the pace needed for such short timeframes. In addition, larger companies are demanding their suppliers and partners demonstrate security, leading to an onslaught of compliance requirements, spreadsheets, and huge questionnaires, all of which are now familiar to the CISOs and security compliance teams who must answer them to stay in business. In this day and age, it's remarkable how few teams address these problems with automation—particularly the privacy, legal and compliance aspects of incident response. Teams across the business need to know what applies to them and subsequently follow the shifting landscape. Our platform was purpose-built to fill that gap, and our regulatory and compliance libraries make it easy for companies to go from no coverage to full coverage overnight. One further recommendation: Don't assume it's taken care of, as there are myriad examples of breached companies where one team thought the other was prepared, but they weren't. Security and legal leaders need to work closely together to stay on top of this, or else it will be expensive chaos when an incident does occur.

TAG CYBER: How does your platform help an enterprise take a proactive, as opposed to reactive, approach?

BREACHRX: Our platform gives teams a place where they can pull together everything needed for an incident. Our customers think of our platform as their incident response hub, and our automated workflows help teams easily pull all an organization's requirements and efforts together into a single system of record that's easy to maintain. We provide our customers with libraries of regulatory and compliance requirements, playbooks, and procedures for a wide range of security and privacy incidents. We also make it easy for customers to capture their cyber insurance requirements, contractual terms, and any other obligation or task that needs to be accomplished if an incident or data breach occurs. This integrated

platform approach makes it extremely straightforward for our customers to demonstrate they have a best-in-class incident response program that exceeds the criteria of many of the top global voluntary and externally audited compliance frameworks, such as SOC 2, ISO 27001, CIS Controls, and NIST CSF. We've built automation workflows and tests for onboarding that guide customers through what's needed to achieve rapid compliance; we've had customers get fully prepared in under a week.

TAG CYBER: You also provide training and practice exercises so a company will be prepared for real-life threats. Can you tell us more about those offerings and how they are different than a traditional tabletop?

BREACHRX: Most companies focus solely on the security aspects of their incident response, and that goes for their tabletop exercises, as well. We hear lots of stories about handwaving the other parts of a response, regardless of the fact that those aspects generate 70% of an incident's cost. With our platform, companies can run cyber exercises and proactive assessments to determine what the impact of various types of incidents would be. It also gets the team well-versed in their procedures, ensuring all parts of the business are ready and prepared should an incident occur. We're big proponents of a "crawl, walk, run" approach to exercises. Many companies want to jump right into a big tabletop ransomware exercise with their executives without practicing beforehand. Our customers scale their simulations up, starting with phishing, stolen laptops, misdirected email, and malware infections, before working their way up to the big exercise, by refining their processes, testing their legal and privacy teams, and more. It's led to great success and more budget, because they demonstrate their proficiency and readiness.

TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security and compliance, along with any advice you might have for practitioner readers.

BREACHRX: A few thoughts here. From a threat standpoint, we believe it's highly likely that attackers will continue to focus on software supply chains to get deeply embedded in their targets. The shared code from open source and commercial libraries is a prime target for threat actors, and we'll most likely see continued attacks with global repercussions moving forward. From a compliance and legal standpoint, a couple of thoughts. At some point we expect to see a lawsuit from a breached company targeting their compliance audit firm for misrepresenting their readiness. It might take a couple of years to come to fruition, but we feel it's only a matter of time. And in the near-term, we expect more C-level executives, including CISOs and CPOs, to be targeted personally by governments worldwide; the recent Drizly action by the FTC is a harbinger of things to come.