A NEW YEAR, A NEW DBIR

A CISO'S PERSPECTIVE

Dr. Lee Mangold, CISSP | CHIEF INFORMATION SECURITY OFFICER, FORTRESS

Since 2008, Verizon has published its annual Data Breach Investigation Report (DBIR) cataloging cybersecurity problem trends from the preceding year. When this report drops, marketing teams around the world rally to see what quotes can be pulled from the report to add to their own marketing materials.

As a CISO, it's a little different for me...

To get the marketing perspective out of the way: Yes, we know the phone calls are incoming, we are prepared to see the DBIR pull-quotes in our inboxes from every vendor out there, and yes, our own marketing team will start asking us to comment and write blogs. *Hi Marketing Team!*

While part of the CISO role is to support the business – to include my beloved marketing team – the impacts of industry reports go a lot further than that. We live this report every day. We see these same trends in our own organizations, and we hear about them from our peers. However, what we don't always see is how prevalent these same issues are outside of our own personal networks and our own choice of news coverage.

One of the key findings in the DBIR – and one that is of obvious importance to my own company – is the sharp increase in incidents relating to third-parties. Verizon reports that **30% of breaches in their 2024 sample involved a third-party – double that of 2023.** Speaking from experience within my own experience and network, I suspect that the number is much higher than that.

Fortress has been a leader in third-party risk management for many years. In that time, we've seen the good, the bad, and the *head-in-the-sand* when it comes to third-party risk. In recent months, we've seen the explosion of new generative AI companies and start-ups hit the scene. Each of them promising to solve all our problems – and most of them have been around less time than it took me to write this blog.

With this new wave of technological breakthrough comes an even greater risk from third-parties. Before the famous ChatGPT, what organization would allow a 3rd-party to consume all its emails, documents, source-code, text messages, chat messages, meetings, into a massive black-box to comingle with other people's data? But that's what happened! Organizations, in a rush to "adopt AI", accepted click-terms en masse and handed over the keys to the kingdom.

> **"Before the famous ChatGPT, what organization would allow a 3rd-party to consume all its emails, documents, source-code, text messages, chat messages, meetings, into a massive black-box to comingle with other people's data?"**

This isn't just about ChatGPT (or any other AI platform). Rather, this is about truly getting back to basics and understanding how those stakeholders you rely on the most are securing your data and whether they will be there for you and your business tomorrow.

In line with that, I have some recommendations *(outside of contacting our sales team, obviously)*:

- **Inventory your vendors.**
  The biggest issue I've seen across all industries in TPRM and SCRM is a lack of rigor around who your vendors actually are.
- **Assess your vendors.**
  Evaluate vendor security postures rigorously during procurement, not just with questionnaires, but through verified evidence and third-party risk management (TPRM) platforms.
- **Reduce the Impact.**
  Segment networks and data to limit the blast radius if a third-party relationship is compromised. Does your Salesforce deployment really need to have access to all your CEOs emails? (yeah, go check)
- **Demand secure practices**
  It's your organization's money and your organization's reputation on the line. If a vendor refuses to meet your standard of security, find another vendor.
- **Plan for problems.**
  Third-party vendors are just like your own organization. They are subject to breaches, availability issues, and economic problems. Plan your response before you need it! That's easy to say, for sure, but most organizations never take the time to think about the simple "what ifs".

There's a lot more to the cyber world than just TPRM, for sure. But TPRM has a position. All the big and important things CISOs are concerned about for our own organizations can be voided out if all of our critical partners don't feel the same way. While the DBIR (and other reports) are typically lagging-indicators, the future message around TPRM is clear: **We expect more problems and greater impact ahead.**

Perfection in TPRM isn't the goal. 100% security isn't a real thing. But you can prepare for the worst by taking action while still hoping for the best!