GDPR: Don't Let the Alarm Bells Shape Your Thinking

By Dane Connell

The European Union's General Data Protection Regulation (GDPR) is beginning to effect real changes from corporate policy to cyber insurance to investments. Conversely, the flow of predictions about GDPR's overall security impact continues to lean toward alarm and disconcert. No doubt, corporate information security professionals are not the only minds contemplating the implications of the GDPR; threat actors of all strains have been eyeing the regulations for possible attack vectors and opportunities since the first published GDPR draft documents. As with all public policy, the GDPR will inevitably result in unintended consequences. However, reports predicting an increase in extortion and obstacles to law enforcement may be missing the mark. While possible, we need to ask ourselves, are these consequences probable and do they outweigh the benefits? Thinking more clearly, which preparations will optimize not just investment and compliance, but effective prevention?

As the GDPR effective date of 25 May approached, there was mounting speculation of increases in targeted attacks demanding ransom of companies found in breach of GDPR requirements. New restrictions on domain WHOIS data is oft-cited as another unintended consequence affecting law enforcement and security researchers. While these outcomes are possible, security professionals need to consider if they are probable given their specific context. Marketing firms certainly need to consider the nature of their data holdings, usage, and the protections in-place. Vendors providing online services have different concerns. To-date, events have not borne-out these dire predictions. Our research has not detected the expected uptick in dark web chatter regarding GDPR. In fact, benchmarking shows quite the opposite. While insufficient in length of time to draw definitive conclusions, we have not seen empirical evidence of a shift in techniques or tactics vis-s-vis extortion activity. Conceptually, it continues to make sense that attackers may eventually leverage the fear of GDPR financial penalties to accelerate extortion in both volume and intensity.

GDPR will evolve as an opportunity to reshape the personal data landscape and businesses will necessarily adapt. While much focus has been on the enforcement mechanisms and potential fines, the fact is businesses around the world have invested significant resources moving their organizations towards compliance – but the effectiveness of those investments remain to be seen. With success measured in terms

of "no news is good news," GDPR is but another compelling reason for information security professionals to do some soul-searching: is your organization sufficiently focused on the basics? With the exception of the most advanced threats, criminals prey on targets of convenience, easy prey. Is your organization nimble in minimizing your threat surface? Do you focus on user-training, or education? Do you have a dedicated staff examining your organization from the perspective of the adversary? After the Y2K-like scramble to GDPR compliance, Q3 2018 might be a good time to step back and examine how well you're executing on the fundamentals of information security.

Inquire here to learn how our Liberty's Triton team can help your company stay ahead and protected from emerging cyber threats associated with GDPR.

Liberty Advisor Group is a mission-focused advisory and strategic consulting firm. *We partner with our clients to solve their most complex business issues and improve enterprise value. Our experienced team has a proven track record in Business and Technology Transformation, Data Analytics, Business Threat Intelligence, and Mergers and Acquisitions. We offer original thinking combined with factual data to develop comprehensive, situation-specific solutions that work. With straight talk and proven results, we accelerate growth, drive efficiency and reduce risks. We are experienced. We are doers. We are Battle-Tested.*