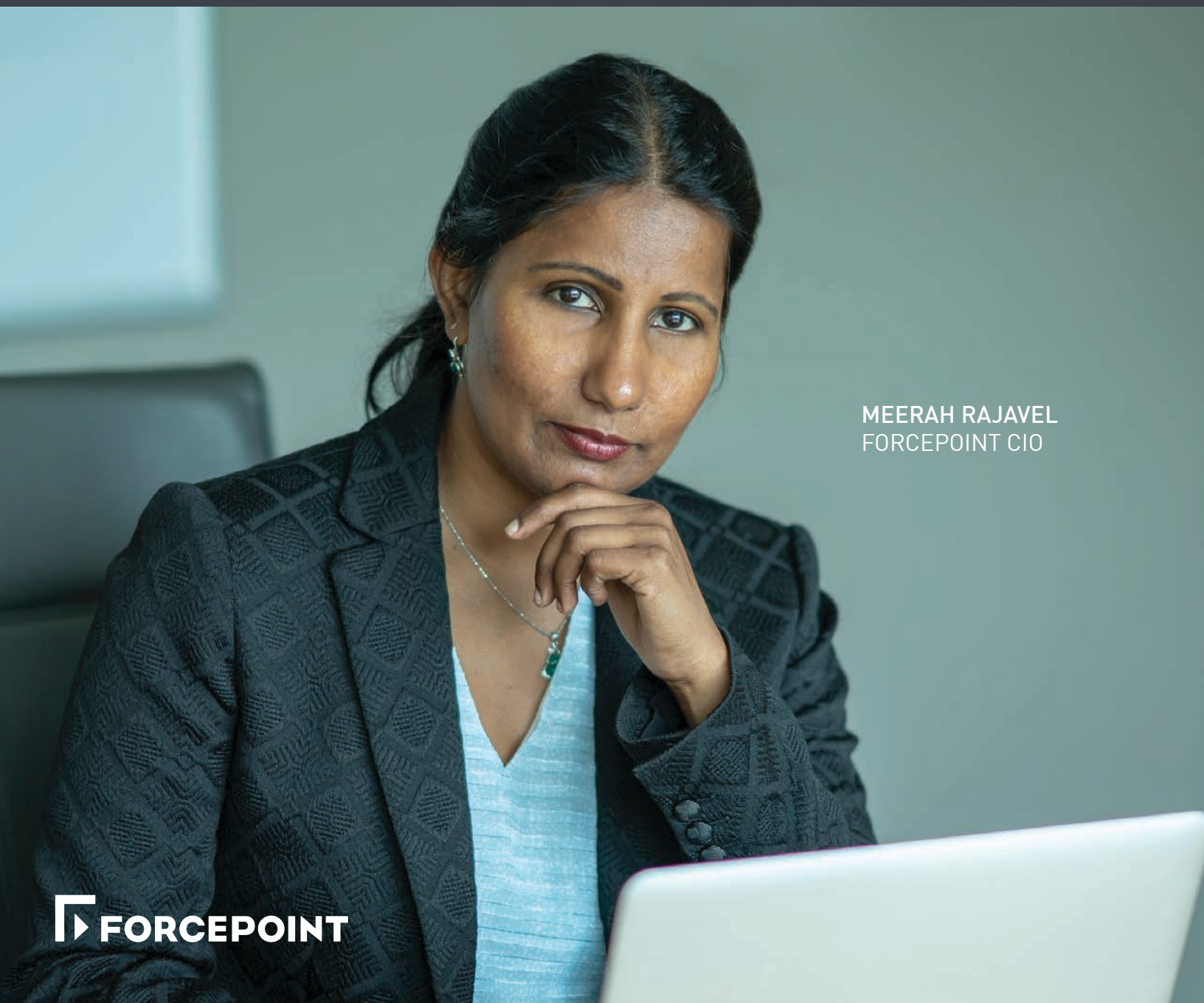
Issue 1 2018

HOW I DID IT.

FORCEPOINT'S CIO ON GDPR READINESS: GET STAKEHOLDERS ALIGNED. THEN EXECUTE.



MEERAH RAJAVEL
FORCEPOINT CIO

FORCEPOINT

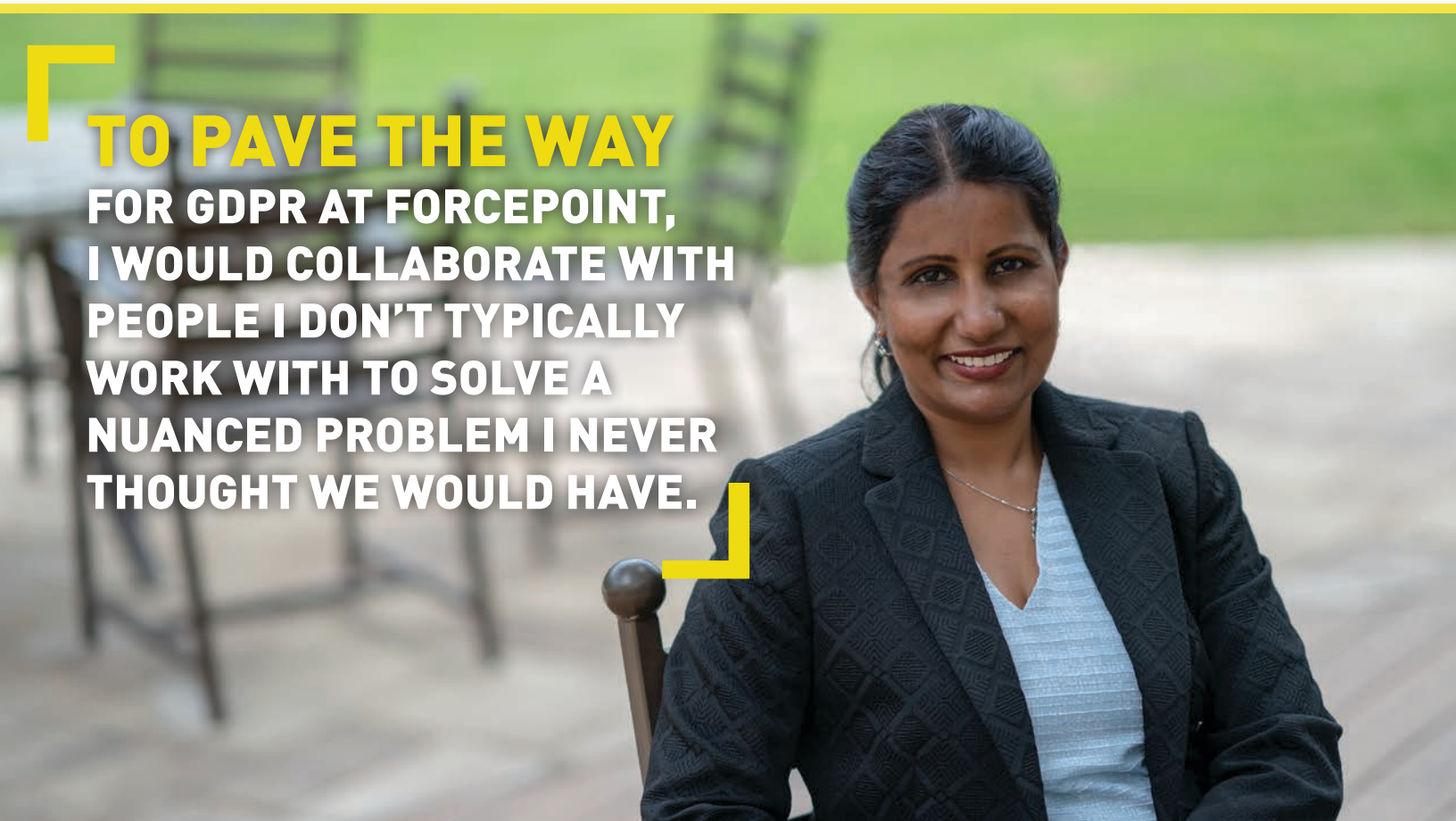
It's not unusual to see the CISO, Head of Human Resources, CIO, and Chief Legal Council meeting in the boardroom. However, it's not the cast of characters you would expect to solve a data protection challenge.

That's what makes the General Data Protection Regulation (GDPR), the latest EU data privacy law, so unique. The first of its kind, the GDPR comprises initiatives designed to protect EU citizen data from a wide range of "offenders," from overzealous marketers to unscrupulous cybercriminals.

The GDPR is naturally far reaching. After all, enforcing this level of data protection for an entire continent is a challenge like nothing we've ever seen before. Every international company and its C-Suite will be impacted, regardless of industry, the city it calls home, or how much personal data it collects.

The GDPR's demands are as clear as day, but the legislation's authors gave us very little on how to go about achieving them. To do so successfully, we risked breaking privacy laws or impacting our company's culture. To pave the way for GDPR at Forcepoint, I would collaborate with people I don't typically work with to solve a nuanced problem I never thought we would have.

In the end, our leadership team would need alignment on legal and security terminology, what the law meant to Forcepoint, and how security technology would be applied to protect personal data.



INTERPRETING THE GDPR'S GUIDELINES

As security professionals, we have a tendency to solve our problems with technology. Yet, in its current form, the GDPR is basically a set of guidelines—not prescriptive rules. Before talking tech, we had to apply meaning to the regulation's guidelines.

For example, the GDPR mentions phrases like "good controls and measures" without defining them. Words such as "protect" don't fully translate, since there are five or more available technologies that do exactly that. Under the GDPR, encryption is "not strictly required" but regarded as important and valuable. It was as if the law's authors were simply telling us, "Do the right things, guys."

Communication is a fundamental building block to GDPR planning. To start down the right path, stakeholders must align on terms for processes and technology. As we moved forward, we realized we needed to continually revisit terms and come to an agreement on their meaning.

KEY FINDING:

Align stakeholders by referring to terms in well-known programs such as NIST and ISO. There is a better chance people will understand terms they have previously seen. Something as seemingly innocent as using an industry term inconsistently (i.e., referring to alerts as events) can cause enough confusion to slow down GDPR readiness.

TEAMING UP WITH HR

KRISTIN MACHACEK LEARY
CHRO, Forcepoint

On HR involvement: I found it necessary to be actively involved from the onset; coming in at a later stage could have potentially derailed our planning. Also, it's critical to speak from a business expertise, not just a functional one. We understand how local laws and regulations relate to our employees better than anyone.

Working together towards a common goal: True collaboration means putting your ego in the back seat—no one stakeholder has the skillset needed to execute an initiative of this scale by themselves.

GDPR's power shift: GDPR has shifted power back to the employee base, yet a lot of the key business protections are not changing. For example, despite the right to be forgotten, if an employee is terminated for a reason more serious than performance issues—misconduct or discriminatory behavior—it will still be flagged by a background check when that person interviews at another company.

Preserving culture while protecting data: We decided early on to flip the idea of how people use company resources. I have no problem with someone paying a bill or checking their social media—it's 2018 after all. We needed to design an effective program that reflects that reality.

FINDING COMMON GROUND

In our first moments of working together, our group gathered around a table, each of us armed with expertise from our respective fields. As we took turns voicing our concerns, I quickly realized something was off—there was a language barrier.

Looking back, it makes sense. We each represent different parts of the business, so it's only natural that we would find certain aspects more important than others. Legal focused on the hefty non-compliance penalties; HR raised concerns about the impact on company culture; I was preoccupied with finding efficient ways to enforce this degree of data protection.

It became clear that if we didn't align, there wouldn't be a successful program. Fortunately, we were able to find common ground, allowing us to jointly determine how the regulation would apply to each part of the business. Communication early and often allowed us to move forward in lock-step when confronting more pressing issues.

KEY FINDING:

It's important to envision how a necessary action on one side of the business might impact another. For example, I learned we needed to make a clear distinction between data collection and monitoring. If we're going to do certain types of monitoring, Legal needs to be sure it won't violate the law, and HR needs to be able to convey it to the broader workforce.

A LEGAL PERSPECTIVE

JOHN HOLMES

General Counsel and Corporate Secretary, Forcepoint

Interpreting the regulation: With regards to GDPR, one of the challenges we all face is that there is not yet a body of interpretation out there to go to. You have the actual regulation, the statements that were made, and quite a few recitals—which may even be longer than the actual regulation. With concepts like "legitimate interest," until you have European courts interpreting what that means in a given context, you don't really know how things will turn out. You just have to give it your best judgment and hope for the best.

Formulating a strategy: Start to develop some familiarity with GDPR principles and let them guide your internal implementation strategy. Do your best with integrity, understanding that compliance is not a zero-sum game—perfection is unattainable. You always have to be improving, always adjusting your program to fit the organization and to remain in alignment as the regulation evolves.

On data collection: Under GDPR, we are required to understand our legitimate interests in any given type of information collection scenario. For example, we collect employee family information, names and birthdays and the like, with the legitimate interest of administering a health insurance program for our employees. Even though it's sensitive information, if we do the right things to protect it, our interest in being able to administer that program and the employee's interest in having such a program outweighs privacy concerns.

MAPPING THE TECHNOLOGY AND CHANGING INTERNAL PROCESSES

The GDPR does not provide a prescriptive path to compliance. Once we had a shared understanding of the regulation's requirements and alignment on how it would affect our company, we needed to figure out the right technologies to apply. At Forcepoint, we created a three-step GDPR implementation process.

1 Identify where personal data resides and map data flows

Most organizations are not sure exactly where their data resides at any given point in time. As data moves beyond the walls of your perimeter, it tends to "hide" in sanctioned or unsanctioned devices and apps.

Our environments are dynamic, so we need to understand not only where data is stored, but also where data is in-motion. As a result, data flow mapping for data at rest (stored), as well as in transit, was a major part of this exercise.

We used data loss prevention (DLP) technology to gather information about our data: the user it is attributed to, data type, where it lives, when it was accessed, and permissions. Combining cloud access security broker (CASB) technology with DLP helped us identify personally identifiable information (PII) as it moved through the cloud. There are solutions in the market—ours included—with simple checkboxes that can adjust policies based on GDPR compliance. Despite these outstanding tools, a great deal of manual work was still required.

2 Protect personal data and detect threats

BYOD policies, mobile devices, and cloud apps have added never-before-seen complexity to security and have expanded the attack surface. We need to see risk in real time, but legacy IT wasn't designed to protect data that travels outside of the enterprise and into the cloud, and it doesn't offer visibility into risky activity as your people interact with data.

To truly evolve security from its current rigid and reactive state to one that is flexible and proactive, we need to harness the continuous monitoring and analytics capabilities available within a user and entity behavior analytics (UEBA) solution.

UEBA allows us to see risk holistically, and when combined with other enforcement technologies (like DLP, for example), we can enforce policies that are unique to the user and only when needed. Instead of locking down productivity, our employees benefit from a layer of protection completely invisible to them. That's something HR will always get behind.

3 Respond quickly and adjust processes

The reality is that threats will make their way into even the best security programs. With the GDPR, organizations must report a personal data breach within seventy-two hours Despite these outstanding tools, a great deal of manual work was still required. That's not a lot of time to react.

One way to get ahead is to have early insight when a user becomes compromised. In the not so distant future, we'll rely on UEBA to surface behavioral anomalies and identify risky user activity. UEBA provides a more informed contextual picture, combining data from traditional security systems, SIEMS, and
DLP tools with that of other organizational sources (e.g., HR, travel logs, email and chat communication).

Once a breach does take place, how do we find out exactly what occurred? Our insider threat tool provides forensics through video collection and playback, expediting investigation and support attribution. In the unfortunate event of a breach, the GDPR's enforcers will want answers; I can't think of a better tool you would want in your possession. We spent a lot of time on procedures and policies with regards to Forcepoint Insider Threat, and this was a key area where we needed HR and legal involvement.

GDPR PLANNING IS UNIQUE TO YOUR ORGANIZATION

Every company will have their own version of GDPR planning and will experience problems that we may or may not have come across. This is where you and your colleagues can build upon your foundation of mutual understanding and work through these issues as they arise.

People often ask me, "How do you know if you're 100 percent GDPR compliant?" The true answer is no one can ever be completely sure. What we can do is communicate often, anticipate where the GDPR may affect the business, and implement the right tech to proactively protect against data incidents. ■

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact