Issue 2 2018

HOW I DID IT.

FORCEPOINT'S SR. DIRECTOR CORPORATE INFRASTRUCTURE ON MOVING TO MICROSOFT OFFICE 365: KEEP ONE EYE ON SECURITY, BUT DON'T LET THE CHALLENGES KEEP YOU FROM THE CLOUD.

RICHARD VINE
SR. DIRECTOR
CORPORATE INFRASTRUCTURE

FORCEPOINT

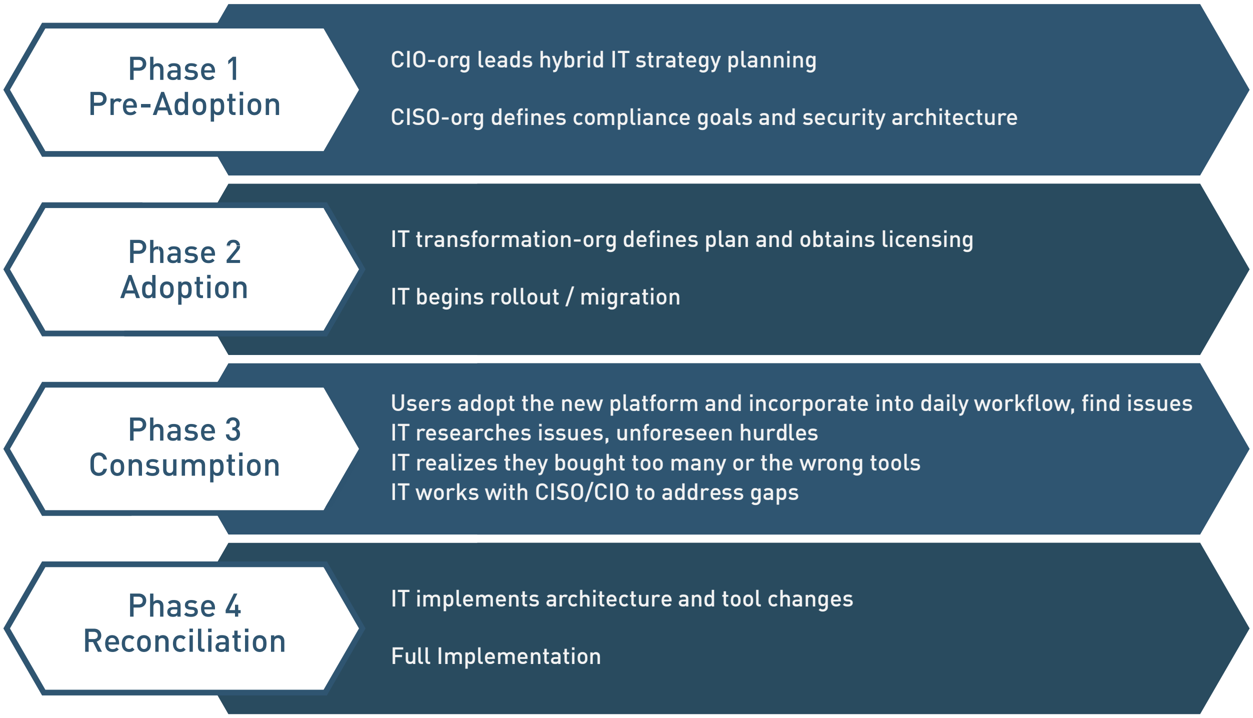
Microsoft said migrating a company of 2,000 employees, let alone a cybersecurity company, to Office 365 in four months would be impossible. But our history made a fast and seamless move a requirement. Forcepoint was formed by combining three established companies, with additional acquisitions coming shortly after. Not only did this bring varying culture, geography, and compliance requirements, but also five different email architectures, nine different conference solutions, multiple collaboration platforms, varying software generations, and a workforce spread across 49 countries.

After evaluating the best way to consolidate and update these disparate tools, we decided to simply skip a generation and move to a solution that provided a more flexible and agile architecture. One that made sense from multiple perspectives like speed, efficiency, cost, and user experience. And one that could not only solve our email needs, but also streamline other key tools. We decided to move straight to Microsoft Office 365.

While many companies think of the move to Office 365 as "moving email to the cloud," it's actually much more powerful than that. O365 delivers a rich ecosystem of capabilities and can provide an entirely new way of collaborating across your business. With that in mind, instead of an email or communication or infrastructure project, we looked at this as a workforce productivity initiative. That meant we had to think about people, their behavior, and security from the beginning. We had to not only ensure a virtually invisible email transition but also prepare for users to find other functionality and start using it. At the same time, we had to maintain the unique security and governance requirements that come with being a security company. And we had to do it within the four months Microsoft said was impossible. ***Here's how we did it.***

OFFICE 365 ADOPTION JOURNEY

Many firms go through a similar journey when rolling out Office 365.



Phase 1
Pre-Adoption

CIO-org leads hybrid IT strategy planning

CISO-org defines compliance goals and security architecture

Phase 2
Adoption

IT transformation-org defines plan and obtains licensing

IT begins rollout / migration

Phase 3
Consumption

Users adopt the new platform and incorporate into daily workflow, find issues
IT researches issues, unforeseen hurdles
IT realizes they bought too many or the wrong tools
IT works with CISO/CIO to address gaps

Phase 4
Reconciliation

IT implements architecture and tool changes

Full Implementation

PILOT PROGRAM WITH IT + VOICE OF THE CUSTOMER

We knew that turning off email or access to essential documents for even one day wasn't an option—our transition had to be seamless. We started with an IT pilot program, including infrastructure, cloud, Exchange, Sharepoint, workflow, and security experts, as the first group to move to Office 365. By limiting the initial migration to just IT, we had an opportunity to work out the kinks and focus on bullet-proofing our security and governance.

Our pilot team was willing to openly discuss issues with each other and take on inconvenience during the transition period when we were maintaining on-prem systems while moving to the cloud. This allowed us to learn from mistakes and address any problems before expanding the project.

However, while critical about technical hiccups, IT users aren't nearly as sensitive to usability and user experience as others might be. I also wanted to hear from users outside IT who would expect high productivity and a smooth experience. We recruited volunteer customers across different departments such as sales, finance and marketing, and in global offices and the field to provide the "voice of the customer." Our legal team, for example, had a unique set of requirements different from the other departments.

Once our trial customers were satisfied, our team began mass migrations with the help of lots of pizza and late nights over a period of six weeks. These usually took place on Thursdays or Sundays to ensure that support was fully staffed the next day to deal with any unexpected issues.

KEY FINDING:

Have the right monitoring and audit functions in place during the transition. When moving through hundreds to millions of transactions per day, the transitory state allows for a possible loss of communication or for security policy rules to send more emails to quarantine, which can surprise users and disrupt productivity. It's vital, from an operations perspective, to start monitoring "then vs. now" to ensure all policies are tuned correctly to lessen the chance of disruption.

SECURITY THROUGHOUT

There is a perception that when you move to the cloud, all of your security needs are taken care of, but that's not the case. Even if you live in a gated community, you still lock your door. Office 365 provides a resilient infrastructure and some level of security, but no cloud company can decide what content is important for your organization nor what your policies should be. To ensure our users and confidential IP were protected, we integrated security and governance right from the start, and the security team was key to selecting and evaluating the solutions.

I am a firm believer in "drinking our own champagne," so we leveraged Forcepoint technologies where appropriate to protect company assets within the Office 365 cloud.

- **Visibility and control:** We implemented Forcepoint Cloud Access Security Broker (CASB) to provide visibility into user activity, data flow, and data security in the cloud and across all endpoints.
- **Analytics:** We aggregated data from Forcepoint CASB, Okta, and the O365 Security Center. We also fed the analytics into our SIEM/UEBA to identify risky users and behaviors and provide advanced incident response capabilities.
- **Protection:** We introduced Forcepoint Email Security for inbound spam/av filtering, and DLP for data protection on outbound emails.
- **Enforcement:** We implemented Forcepoint Dynamic Data Protection to enforce policies in near real time when there is risk of a data loss incident.

Essentially, our security approach follows our risk-adaptive protection framework model, which enhances user productivity through controls that react to high-risk users and activities instead of imposing one-size-fits-all restrictions that constrain all users.

KEY FINDING:

Plan to manage security in a hybrid ecosystem: cloud and on-premises. Though we included security early on, I wish we had done more systemic design thinking about the transitional phase. In our case, during the four-month rollout we had to deal with an overlap of both on-premises and cloud, and some of our security design did not naturally fit the hybrid mode. This complicated operations during the transition period.

PLAN FOR UNWANTED SURPRISES

Despite our preparation, we did have a few surprises crop up.

- **Change management was key.**
  We learned that it was important to foster buy-in from departments and stakeholders across the organization at the beginning. Email was considered a lifeline system for the business, so everyone had an interest in making sure the solution and rollout were a success.
- **Planning for unexpected complexity is a requirement.**
  We found that shared mailboxes across the company required more flexibility in the migration process than we foresaw. Individuals on various teams were accessing all or parts of shared mailboxes, which meant we couldn't split and schedule the migrations cleanly by teams. For example, we couldn't say, "Sales moves on this date and Engineering on that date," without taking into consideration mailboxes that spanned across the two groups. This increased the complexity and sometimes affected users that were surprised by the earlier date and not ready for the transition.
- **During the transition state, prepare for limited monitoring.**
  Some tools were not able to deliver full functionality when the data was split between on-premises and cloud systems. We didn't have full CASB usage until all users and data were migrated.
- **Understand the impact of new capabilities.**
  We held training on some of the new capabilities, but some training we intentionally held back. That didn't stop users from finding and beginning to use the applications. In retrospect, it would have been better to communicate all the functionality up front to better prepare users.

KEY FINDING:

Be ready for users to find and use new tools. Many IT organizations roll out Microsoft Office 365 focusing security planning on email, calendar, and IM with the idea that users will ignore other tools like Teams and Sharepoint. We never announced Teams, yet our users discovered and began utilizing it.

A common mistake is not preparing security for these capabilities, which typically require very different design from email. Plan for this at the start of the project, and be prepared if your users embrace new capabilities organically.

WHAT THE FUTURE HOLDS

Going forward, this migration provides an opportunity to look across the company at how we communicate and collaborate holistically. If everyone is sitting on their own island, we can end up with pockets of application use that don't translate to company-wide collaboration. Office 365 gives us the chance to eliminate duplicate and risky services and move toward maximizing total cost of ownership (TCO), not only from a direct cost point of view, but also from an increased productivity perspective. If users don't have to visit five different document management platforms, potentially one for each department, their work lives are much less complex. We're evaluating this now.

There are also other capabilities, such as the Yammer social platform, that we haven't promoted and users haven't adopted on their own. We're looking at activating usage of those. There are older versions of Sharepoint throughout the company as well, because it was previously a separate platform. With Office 365 we have a chance to migrate documents to a centralized space with the most recent version. We're also having conversations about how Office 365 capabilities could replace some "Shadow IT" as we now offer the same functionality in a sanctioned platform. At the same time, we're evaluating how to best accommodate other applications in addition to Office 365, providing some amount of user choice.

DON'T ASSUME THAT BECAUSE YOU'RE GOING INTO THE CLOUD THAT SECURITY IS TAKEN CARE OF.

LESSONS LEARNED

In the end, I was pleasantly surprised by how positively users embraced the move to Office 365. Our IT team did have a little bit more learning to do than I expected, but that was mostly because of the complexity involved as a cybersecurity company with government customers.

To recap, these are the key security takeaways for CISO/CIOs to remember:

1 Don't assume that because you're going into the cloud that security is taken care of. You must define the specific security requirements and policies for your company, regardless of the cloud app. Compare the security features they provide versus your requirements, and plan how to fill the gaps. Email, for example, may not be protected from phishing or spam control unless you implement that protection.

2 Make sure your data is protected per PCI, GDPR, and other compliance requirements. You must have visibility and control over sensitive data.

3 Don't wait to think about the big picture for security until you hit a bump in the road. Bake it in from the beginning and, wherever possible, be risk adaptive and automate enforcement.

There will always be unexpected issues, but with planning, a collaborative team, buy-in across the company, and an end-to-end view of security, you can overcome challenges to deliver a powerful collaboration platform for increased workforce productivity.

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