CloudTweaks

Q&A Between Anthony Park and Dr. Nathaniel Borenstein, chief scientist, Mimecast

1. In your own words, please describe Mimecast and the company's service to readers.

Mimecast is a cloud-based email management company. We provide our customers with a unified solution for their company's email that incorporates security, business continuity, storage, and eDiscovery solutions. With Mimecast, companies' email systems are more secure, less costly and easier to maintain as several different products can be replaced with one holistic cloud-based solution.

In the future, we expect to provide similar services for additional types of information management.

2. What are the key questions most of your customers ask related to security and back-up concerns?

The most common security and backup questions/concerns in the industry are typically related to data access and continuity—who can access data and how do you ensure that there are no service interruptions. Specifically, we've seen questions around:

- **Confidentiality of Data**: How is data encrypted and how much access does staff have to that data? It is important for vendors to create an impenetrable wall between its customer's data, its employees, and other customers' data.
- **Protective Controls Around the Data**: Customers want to know details about how data is protected, including encryption, perimeter security (firewalls), physical security (at the data center) and operational security (change control, incident management, log auditing, staff vetting, *etc.*);
- **Jurisdiction of the Data**: Will the customer breach local regulations or legislation by having data leave the country of origin? And if this is the case, how can my service provider or vendor help me prevent this from happening? Are there multiple locations or ways that data can be stored locally to mitigate this problem?
- **Judicial Access to Data**: What happens when law enforcement requests access to customer data held on a vendor's system under laws such as the US PATRIOT Act or UK Regulation of Investigatory Powers Act?
- **Continuity of Service**: How does my vendor guarantee that my business does not have any service interruptions? It is important to many companies that their service provider has several geographically dispersed data centers and layers of redundancy to protect against an outage.

3. How do you internally insure that client data can be restored if you yourself are subject to a major threat to your datacenter(s)?

The entire Mimecast service platform is engineered with high availability in mind - from the multiple data centers to the design of the internal proprietary protocols.

Mimecast utilizes a grid computing model which is comprised of multiple geographically dispersed data centers, each containing multiple grid nodes (servers) which themselves contained multiple disks. Each customer's processing and data storage is balanced across a number of nodes to increase performance and redundancy, which itself is duplicated across multiple data centers.

This architecture allows Mimecast to lose a disk, a server, a cluster or an entire data center without impacting customer data or service availability.

4. How do you address internal security issues on your platform? What safeguards are in place to guarantee cutting edge processes for a security policy that addresses customer needs?

Managing security for a service provider is not vastly different than managing information security for any other type of company. In fact, the steps are essentially the same:

- Define scope;
- Define acceptable risk;
- Assess risks;
- Treat risks that are beyond the acceptable tolerance;
- Monitor and ensure risks are maintained below an acceptable level;
- Rinse, repeat (as risks change over time, this is a continual process).

The only difference is in that in the first step, you need to ensure that you include the service delivery platform in your risk treatment strategy (it is surprising the amount of service providers who do not include their service platform in the scope of their information security management systems).

You also need to ensure that your level of acceptable risk (as defined in the second step) correlates with the risks your customers are willing to accept. It is important for customers to make sure that their service provider has a compatible scope or level of acceptable risk before choosing them.

While the economies of scale that a service provider offers in terms of proactive information security management is often way beyond that which could be achieved by individual companies themselves, this has to be balanced with the fact that service providers represent a much more attractive target to attackers.

Professional associations such as the Cloud Security Alliance and Cloud Audit are establishing a set of best practice controls and audit mechanisms for cloud service providers that should help customers feel safe with their choice.

Mimecast is a member of these associations and aligns with other best practice standards such as ISO/IEC 27001:2005 and ISO/IEC 20000:2005, ensuring that the company takes a risk-based approach to treating the threats to both customer data and Mimecast data.

5. When major players jump into the market with enormous resources both in development and marketing how does a small start-up protect a market share or niche today?

Being smaller is both an advantage and a disadvantage. Big companies can massively outspend little ones, but little ones can work much faster, and can afford to focus – at least initially – on smaller niches. (Success in only one niche is failure for the big company, but a beachhead for the small.)

So the key is to direct your relatively meager resources to take advantage of your strengths and avoid the kind of head-to-head conflict you're bound to lose. A good first strategy is to exploit your advantage in speed to make sure your product stays ahead on features. That can carry you a good long way, but eventually the product category will mature enough to allow the big competitor to catch up on features. That's why you need a second strategy, executed at the same time as the first, that allows you to move into adjacent markets as well.

This is where I've seen many small tech companies break down. They may be doing a great business in their niche, but if they aren't able to enter a second market, it's more or less a matter of time before a competitor or acquirer takes them out. The great entrepreneurial frenzy at the base of the tech pyramid reflects the fact that each new technology is, initially, a new niche, and therefore suitable for an innovator. Over time, however, the more mature the market, the larger a company seems to have to be to compete.

For the little company, this means that "protecting market share" can be equivalent to "die more slowly." If its sole market niche is consolidating, the small company nearly always has to grow, get acquired, or die.

(Nathaniel)

6. Is there room in the "cloud" for small start-ups and how do they position themselves against the competition?

I think there is, but not if they define themselves in terms of competing directly with the bigt cloud companies. That's like a start-up deciding it's going to take on Visa, or Walmart. The good news is that the nature of large companies pushes them towards the most general, big-market services, so the little guys can find opportunities in more specialized markets. A few of the little guys find that their specialized market is connected to a much larger emerging market; this gives them the rare shot at becoming big companies themselves.

To pick a fanciful example, imagine a company that wants to compete head to head with gmail – same demographics, similar features, etc. They'd have a tough, uphill battle. However, what if they thought they had a clever idea that would make them irresistable to gmail-using dentists? Being small, they could quickly implement their idea, and could better afford marketing to dentists than marketing to everyone. If they're right, the dentists would flock to them, and they could then begin to ask, "what other groups might find this feature useful?" If they can out-invent Google for long enough – an unlikely possibility, to be sure – they might eventually come to rival gmail, without ever having attacked them head-on.

Moreover, for the somewhat less ambitious very small company the opportunities are unprecedented. Using Amazon's cloud, for example, a single programmer could build a specialized cloud service and get it up and running for an incredibly small amount of money. Lots of other big cloud services will eventually create similar ecosystems for small innovators. It would not surprise me if there were thousands of very small companies offering highly specialized services a few years from now, some of them virtual one-man shows operating highly reliable services on a global basis.

(Nathaniel)

7. In terms of current market issues how does your firm determine pricing to attract new customers and retain existing one?

Pricing truly depends upon the variables of each customer's particular situation, the services they want and what amount of information or processes are being moved to the cloud.

8. What issues determine how you address platform reliability and performance from the perspective of your application offering?

I've always felt that if you aimed for 99.9% reliability, you were more or less promising to fail one time out of a thousand. These sort of numbers are necessary and good for SLA's (Service Level Agreements) and the like, but not for the people really tasked with making the system actually work. If you find a bug, you don't ask if it will occur less than 0.001% of

the time; you fix it if you can. I don't care how Quixotic it sounds, your fundamental posture has to be a Zero Defect policy. The system should always work well enough to provide the necessary services, period. I think that's the application-level perspective.

From inside the service delivery team, of course, things look rather different. You have to be proactive in anticipating the effects of growth and the need for additional servers, disks, and other resources. You have to be constantly evaluating your build/test/deploy process, which is ideally a never-ending story of continuous improvement. Basically every issue you can imagine matters, and which one to address next is a tough, one-of-a-kind decision each time.

Having said that, however, no matter how good you are, there are always things outside your control. Perhaps an ISP between you and the customer is behaving erratically, or is down entirely; it will not be obvious to most customers that this isn't your fault. Recently we had a case in which a major vendor released a new version of its software with a bug that caused it to send out email with gross violations of the email standards, causing our system to handle it poorly. Only an acknowledgement from the offending vendor would convince our customers that we weren't the ones being unreliable. (And of course, we hacked around it to ameliorate the problem far faster than the vendor's release cycle.) In this case, little old Mimecast behaved much more "reliably" than the big old trusted vendor, but probably got more complaints from its customers. It's just not uncommon for upstream errors to cause downstream problems.

(Nathaniel)

9. With new announcements daily we see the major players continue to validate cloud applications. How do you protect or at least anticipate a market share niche with the incredible speed of change in today's market?

This is pretty similar to question #5. We can move faster than the big players, but not in more than 2 directions at once, most likely, so the key is deciding which direction to move. There is always another niche, or an adjacent product that you can move into fairly seamlessly, but it's really hard to tell which of those niches will pay off. But basically, I think you have to aim at growth, not niche preservation, acknowledging that your current niches may shrink over time, and using them as a jumping off point.

(Nathaniel)

10. There are many legal and regulatory guidelines dealing with domain names and management. Are there sufficient legal and regulatory processes in place to protect

customers who have made the decision to move all or part of the company data to a cloud platform?

Regulations and legislation can differ based on the geographic location and even vertical market segment of the customer – for instance some of our customers are subject to national legislation such as the UK Data Protection Act that embodies EU Privacy Directive 95/26/EC, which relates to securities investment information; while others based in the state of Massachusetts may be subject to local state legislation such as 201 CMR 17.00 that governs the protection of personal information by those that store it.

With regards the compliance requirements of customers, Mimecast simply operates as a service provider providing a platform for customers to conduct their business in accordance with their own compliance requirements. Mimecast designs its service delivery platform and conducts its business with consideration for its customers' compliance requirements, but, like most cloud platforms, does not have a direct effect on whether a company is compliant or not—that still remains in the hands of the companies themselves.

11. What is the new paradigm of cloud business models if any? Put your "futurist hat" on and describe how you see the "cloud" evolving over the next ten years?

I think there are two directions we could go, and the key issue is one you hinted at with your earlier questions: how much, and how quickly, will the industry come to be dominated by a small number of big companies?

In one vision of the future, there will be 1 to 3 cloud companies. Each of them will do more or less the same things, and will create powerful incentives for their customers to do everything with the single vendor. They will have some incentive to innovate to differentiate themselves, but they'll do so slowly and painfully. Mostly they'll imitate each other while crushing smaller innovators.

In another version, there will be hundreds or thousands of cloud vendors, accessed via marketplaces similar to the Android or iPhone Markets today. Those markets will access reputation information about the vendors of services from reputation brokers, so that you'll be able to know a lot about a service provider before you ever sign up; even though it may just be a guy in his apartment in Topeka, you'll be able to see that his customers all adore him. And you'll know that his actual services are running on a third-party service like Amazon's cloud, so that it's professionally administered and reliable.

It's no doubt obvious I prefer the second scenario. The question is, what will make one or the other of these prevail? The answer, I think, is a combination of technical, market, and political factors. Technically, the development of open reputation systems and some related infrastructure is an absolute prerequisite for the happier scenario, and there are others.

From a market perspective, is there really room in the market for all those different little services? And politically, how quickly and how completely will governments allow cloud vendors to consolidate markets before they intervene in the name of antitrust?

Whatever happens, I've little doubt that most applications will move into the cloud. I hope that turns out to promote diversity in applications and vendors, but I can just as easily imagine it going either way.

(Nathaniel)

12. In what way does your internal new product development interface with the need to keep a dedicated cloud security team involved and engaged in anticipating vulnerabilities in security?

Security can't simply be bolted-on, or else it becomes expensive, intrusive and often, ineffectual. Security is a culture, a mindset and a continual process that needs to be integrated into the operational functions of the business, whether that function is product management, development, testing or operations.

Mimecast ensures that the potential risks (in terms of opening new potential vulnerabilities or exposing new threats) are considered early on in the functional specification and design stages of new features. This helps to ensure that controls can be architecturally baked into the final solution early on in the process and that instead of being expensive, intrusive and ineffectual, security solutions are proportionate, integrated and effective.

13. One the key issues related to cloud SaaS applications is the complexity and management of the platform. How has your firm addressed user training and support?

I was a bit surprised, when I joined Mimecast, at the resources we're putting into these areas, but I've quickly come to see how sensible it is. Being proactive is key – teaching people up front can save dozens of support calls down the road, with higher user satisfaction.

Because a cloud service doesn't have release cycles and support issues like those of traditional software vendors, it's fundamentally easier for a cloud service to evolve in positive ways. Key to that, I think, is for the user-facing staff (training and support) to have a clear line of communication with the technical team. This leads to quicker improvements which obviate common support situations, and you can get into a virtuous cycle of quick improvements and quick feedback. I'm not saying we're completely there yet, but you can at least see the outline of that virtuous cycle in what we do today.

Complexity is a hard, hard issue. We're lucky in that most of what we do is well-understood, but we still have a disturbingly large number of configuration options. I think that for the foreseeable future, companies that move to cloud services will see IT savings, but won't be able to get their IT staff down near zero, precisely because of the complexity of configuring all of these services.

(Nathaniel)

14. Can you describe for me your role at Mimecast and how your past background helps the company succeed today?

Well, I'm new enough to Mimecast that I have to say the jury is out on how much I'm helping. Our CTO, Neil Murray, is a superprogrammer, and prefers to focus on the development and deployment of our technology as its user base continues to grow rapidly. So that leaves me responsible for more or less everything else on the technical side. I'm worrying about long term strategy, research and prototyping, intellectual property, standards, and technical outreach and evangelism. I hope to help in all of these areas, but what I think is most important is helping the company move into adjacent markets, to make sure we grow in breadth of offering as well as number of customers. Choosing which directions to move, and when, is probably the most important decision we face, and it's a major focus for me.

This is more or less a perfect job for me. I've played a pretty wide range of roles in the Internet industry in the past, which I hope gives me a broad enough perspective for this role. I think I still have a lot of the idealism of a researcher/inventor, but it's tempered by my experience in multiple startup companies, not to mention IBM. Mimecast is at a very interesting stage – it's grown large enough that you can't really call it a startup, and it needs to pick up some aspects of a big company while preserving its fast-moving, innovative traditions. Between that and the strategic decisions we'll need to make, Mimecast seems to me to be a fascinating place where I have a chance to make a big difference in the long term.

(Nathaniel)