Case Study

mimecast

pib Group

MARKEN
a UPS Company

Cybersecurity and Microsoft 365: Industry Experts Discuss Tight Budgets, Reduced Complexity and Balancing Risk

As the pandemic accelerated digital transformation for businesses across the globe, the move to hybrid and cloud environments kept security experts on their toes. Many companies deployed Microsoft Office 365 (M365) to keep teams connected to accommodate the increasingly remote workforce. The effort to ensure business operations ran normally made productivity and collaboration a top priority, while cybersecurity became an afterthought. This means a large volume of businesses rolled out M365 without implementing proper security measures – prompting the Department of Homeland Security to issue an alert providing security advice to any company pursuing an M365 deployment.

With such rapid change, how are the business world's best security professionals protecting their companies? In September 2021, Mimecast hosted a panel of experts to discuss the potential cybersecurity risks of mega-platform providers, the gaps that exist and how to build a cyber resilience strategy.

At a Glance

With more than 200 million monthly active users, Microsoft Office 365 dominates the critical IT infrastructure of businesses worldwide.

Problem

The pandemic caused a dramatic acceleration of digital transformation efforts, including the rapid adoption of cloud productivity suites, such as Microsoft Office 365. This quick migration has increased risk to businesses, particularly regarding email security. As a result of tight budgets and limited resources, many companies have moved away from the best practice of layered security and centralized protections with a single technology provider instead. To ensure their businesses remain safe, IT and security personnel must learn about the cybersecurity risks of mega-platform providers, the gaps that exist and how to build a cyber resilience strategy.

Solution

- Mimecast Email Security with Targeted Threat Protection
- Mimecast Internal Email Protect
- Mimecast Threat Intelligence

Benefits

- Decreased risk exposure
- Feature-rich email security solution that enables the IT team to implement an ironclad email security strategy
- Protection against phishing, impersonation, and other email-based threats
- Outstanding email protection that is constantly up and running
- State of the art protection that evolves with changing threats and needs
- Superior customer support available 24x7x365

Meet the Experts

J. Peter Bruzzese, Co-founder and Chief Content Officer at ClipTraining (x8-awarded Microsoft MVP)

J. Peter is a global security advisor and technical speaker, an internationally published author, a journalist and an 8x-awarded Microsoft MVP (for Exchange/Office 365).

Jason Ozin, Group Information Security Officer, PIB Group (Current Mimecast Customer)

Jason is responsible at the group level for information security, cybersecurity, data governance and compliance.

Tony Clarke, Vice President of Information Security and IT Operations, Marken (Current Mimecast Customer)

Tony provided IT and security services to several organizations across a wide variety of industries before specializing in healthcare. Previously, he was Head of Information Security at ICON Clinical Research, where he led a global security team and won several cybersecurity awards.

M365 and Managing Risk

Security teams are working to prevent ever advancing cyberattacks while facing tight budgets and limited resources. Because the pandemic exacerbated the need for businesses to wield a cloud productivity suite such as M365 and Google Workplace, Bruzzese saw IT teams making quick deployments, often before they were ready.

"My biggest concern is that people moved to a platform they don't know," he says. "When you're on-premises, you know your environment, you know what your servers can and can't do, you've put the effort in to enhance those servers. We typically surround Exchange on-premises with solutions to bolster security, archiving and so forth. The concern is folks move to M365 without knowing what features exist, don't exist, where the gaps are, and how to plug those gaps."

At PIB Group, the company has been expanding rapidly through acquisition. As their security head, Jason Ozin has quickly become an expert on M365 deployments to ensure his company doesn't fall victim to attack. "Bad adoption of a cloud platform is probably your worst nightmare," he says.

"When we make an acquisition, if they are not on M365, we will move them to M365 and Mimecast straight away. It's our suite of armour that we put around email. Once I know I've got them in M365 with Mimecast protecting them, that's one risk out of the way. Having Mimecast on top of the M365 offerings is very helpful."

Building Cyber Resilience

While the rapid shift to the cloud has caused many companies to centralize protection through a single technology provider, Ozin has remained true to the industry best practice of layered security. "When we adopted M365, we looked at what it could offer us out of the box but knew we would still want a second layer of security," he says.

"Microsoft security is world-class, but too often you look at a feature, and in two months, it will have changed. It's tough to keep up. It's hard to know whether you're getting the best toolset from your investment. Having a secondary layer that does what it says on the tin and is consistent is very important to us. That's why we chose Mimecast – because it's best-in-class."

Echoing the need for multiple security layers, Marken's Tony Clarke illustrated the importance of proactive security and finding partners you can trust. "From a pure security architecture point-of-view, I can't imagine not having two layers of security.

Given the volume and variety of threats, you might get away with using just one layer, but sooner or later, it will cause a problem. Adding a second layer is really about risk reduction and being proactive with your security architecture." After it bolstered Marken's security architecture, Clarke highlighted his appreciation for Mimecast:

"Mimecast is a straightforward solution. Its API-driven nature makes it easy to orchestrate. Not to mention actually getting a return-on-investment through the experts at Mimecast. It really does feel like a partnership model where someone is trying to help you consistently to get the best out of the solution and the service."

Avoiding "Good Enough"

Facing limited resources and budgetary constraints makes it difficult to ask for more when purchasing security solutions. Bruzzese refers to this as the "good enough" mindset and says it is one of the most critical things security professionals need to overcome when configuring a M365 environment.

"Maybe because of budget or limited resources or decision-makers not wanting to invest, it feels like more people are settling into this mindset of 'is it good enough?' There's a lot of things in my life where 'good enough' works just fine. But not with security. When comparing solutions, there's a big difference between seeing features checked off and understanding their efficacy. Whether it's EOP and Defender for 365 (formerly ATP) vs. a third-party solution like Mimecast, you need to know their differences."

"Mimecast is a straightforward solution. It's API driven nature makes it easy and straightforward to orchestrate. Not to mention actually getting a return-on-investment through the experts at Mimecast. It really does feel like a partnership model where someone is trying to help you consistently to get the best out of the solution and the service"

Tony Clarke

Vice President of Information Security & IT Operations, Marken

Convincing Decision Makers

Perhaps the most challenging thing for security professionals is getting executives' and decision-makers' approval to purchase additional security tools to shore up defenses. Those who aren't well-versed in security may not understand the need to layer on top of M365 or another platform when it comes to innate security functionality. For Ozin, the key to reaching the decision-makers is through storytelling.

"Fear, uncertainty and doubt (FUD) don't work, or they only work after your business' security has been compromised. Rather than attempt to scare executives, I prefer to explain what could happen, what has happened to competitors, and what we would do if a crisis occurred. Running through desktop exercises where we show different scenarios are really, really useful. It's a way to get people to think about the reality of a situation. Storytelling is a handy tool for me."