

BLG

# BLG's Cyber Resilience Journey with Mimecast

“The lifeblood of a law firm is email and document management, you can turn everything else off, but without email and document management, we do absolutely nothing.”

- Wayne Cross, Director of Cybersecurity and Infrastructure Operations at BLG

## Customer Success Highlights

- Reduced successful phishing attacks
- Increased phishing simulation detection and reporting
- Enabled automated response workflows

## The Challenge: High-Value Targets, Legacy Defenses

As Canada's largest full-service law firm with more than 200 years of history, Borden Ladner Gervais LLP (BLG) handles some of the country's most sensitive legal work—spanning corporate finance, banking, intellectual property, mergers and acquisitions, and more. That makes the firm an attractive target for cyber attackers, and it makes email the firm's most critical—and most vulnerable—asset.

Two watershed events in the legal industry sharpened BLG's sense of urgency. The first was the Panama Papers breach, in which a promin released worldwide.

The second was a devastating ransomware attack on one of the largest law firms in the world, which encrypted over 60% of the firm's assets, started in Europe, and rolled across North America before employees even arrived at work.

“That shook our legal leaders significantly,” Cross recalled. “It made us take a very deep look at how we are protecting our most precious asset.”

BLG's existing email security tools were fragmented and aging. Cross and his small three-person team needed a unified, proactive platform—one that could block threats before they reached users, integrate with the firm's broader security ecosystem, and operate silently enough that lawyers could work without disruption.

## The Solution: Why BLG Chose Mimecast

Cross and his team began researching how the world's largest law firms were protecting their email environments. One name came up repeatedly: Mimecast.

**“When law firms got breached because of email, they went to Mimecast, we decided it was in our best interest to move to Mimecast before we got breached. Today, it forms the cornerstone of our email gateway protection.”**

- Wayne Cross, Director of Cybersecurity and Infrastructure Operations at BLG

### **A Partnership from Day One**

When BLG began evaluating Mimecast in 2019, there was one obstacle: Mimecast did not yet have a Canadian data center, and BLG’s clients—major banks and insurance companies—required their data to remain in Canada. Rather than walk away, BLG and Mimecast forged a partnership. BLG committed to being the beta customer for Mimecast’s Canadian infrastructure, and within three months, Mimecast had approved and begun building out its Canadian presence.

“The proof of concept was so successful, we just switched it into production,” said Cross.

Several capabilities made Mimecast the clear choice for BLG:

- **Pre-delivery threat protection:** Mimecast’s gateway blocks phishing, malware, and targeted attacks before they ever reach the mailbox. “We appreciate the in-line scanning that Mimecast provides,” Cross said.
- **User empowerment:** Mimecast’s tight integration with Microsoft Outlook gave BLG’s lawyers self-service tools—such as the ability to block unwanted senders and report suspicious messages—without disrupting their workflow.
- **Rapid administrative response:** When a threat does slip through, Mimecast gives BLG’s administrators the ability to pull emails from mailboxes and escalate filtering policies in minutes, not hours.
- **Seamless compliance and archiving:** With clients in highly regulated industries, BLG needed robust e-discovery and data governance capabilities. Mimecast’s integrated compliance tools met those requirements without adding complexity.
- **Silent deployment:** For a firm where lawyers resist any change to their workflow, Mimecast’s low-friction deployment was essential. “The tools we need have to allow the lawyers to work the way they want to work,” Cross noted, “Mimecast fit that bill.”

### **The Results: Measurable Risk Reduction and a Culture of Security**

Within the first year of deployment, BLG achieved a greater than 90% reduction in successful phishing attacks, significantly lowering incident response workload and the risk of data breaches.

### **A Security-Aware Workforce**

Mimecast’s Security Behavior Management program transformed employee behavior. Phishing simulation detection and reporting rates climbed from under 30% to over 80% in less than 12 months, turning BLG’s workforce from a vulnerability into a line of defense.

### **A Three-Person Team with Enterprise-Grade Protection**

Cross credited the Mimecast partnership model with enabling his lean team to punch far above its weight. “If you’re asking me how big my email team is, it’s as large as the Mimecast team plus my team. We don’t manage Mimecast alone—they’re actually an extension of our team. If we call, they answer. If we have an issue, they’re there.”

### **Integrated Ecosystem Defense**

One of the most significant long-term benefits has been Mimecast’s integration with BLG’s broader security stack, including CrowdStrike for endpoint protection and Netskope for cloud security. Cross described the value of this integration:

“It’s quite possible for us to have an email flagged in Mimecast and then execute tasks outside the Mimecast environment. We could block a website with Netskope because a user clicked a link in an email. We could isolate a machine with CrowdStrike because of an email triggered in Mimecast.”

This two-way, cross-platform integration enables automated response workflows that are critical for a small team defending against fast-moving threats. “Platforms can no longer exist on their own,” Cross said. “No one vendor can do it. It’s a team sport.”

### **Preparing for the AI Threat Landscape**

Looking ahead, Cross sees AI-powered threats as the next frontier—and a reason to deepen the Mimecast partnership. Attackers are using AI to craft flawless phishing emails that bypass traditional defenses. BLG is now participating in Mimecast’s AI-driven behavioral analysis program to stay ahead.

“The perpetrators are getting way more sophisticated, so the controls we have must keep up. It’s really important for tier-one vendors like Mimecast to continuously innovate, because anyone can use the same tools to understand how defenses behave and find ways to get around them.”

### **Advice for Other Law Firms**

When asked what he would say to another law firm considering Mimecast, Cross is direct:

“If you are choosing an email gateway, you need to understand your existing ecosystem and ensure that the vendor you’re working with integrates with the tools you currently have. You also need a vendor that is constantly innovating and understands how the threat landscape is evolving.”

He adds: “We consider our law firm top tier, the best of the best in Canada. So, we leverage partners like Mimecast to ensure we are working with the best of the best—because cybersecurity is not our strong point. Litigating is.”

## **About Mimecast**

### **Secure human risk with a unified platform.**

Mimecast’s connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscape, you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.