Protecting the infrastructure and information that handles millions of trades involving $4.7 trillion each day and delivers over one billion investor communications annually is no mean feat. But this is exactly what Broadridge Financial Solutions, Inc. does every day. “Security isn’t an afterthought, something we do in retrospect,” notes Frank McGinnis, the company’s vice president of Corporate Information Technology. “It is ingrained in nearly everything that we do.”

Founded as the brokerage division at ADP in 1962, Broadridge provides investor communications and technology-driven solutions to financial services and corporate firms, enabling them to focus on running their businesses. When ADP spun Broadridge off as a separate entity in 2007, the new leadership team began looking at ways to drive greater levels of cost efficiency while evolving and expanding the company’s solutions portfolio.

The changes in business did not distract from the firm’s focus on protecting system availability and highly confidential customer information from external and internal threats. Rather, it heightened awareness. “We are very much committed to the service-profit chain and aspire to be a leader in protecting customer interactions and information through optimized risk management,” McGinnis says.

McGinnis, who joined the company in 2004, has seen the business more than double in size during this tenure. At the same time, the severity of the threat landscape has intensified dramatically. “It’s been an exciting time to see the company grow and evolve,” McGinnis states. “IT is an important enabler in this process—from innovation in the data center and our systems to risk management programs.”

**Security standards drive technology innovation**

Following the spinoff from ADP, McGinnis and his team of more than 55 IT professionals spent the first couple years focused on integrating and synergizing...
systems and teams. “As part of our effort to gain efficiencies of scale, we adopted a shared services model,” he says. “We’re able to leverage the purchasing power of the larger enterprise to bring about change and do things in a more integrated fashion.”

Broadridge’s Technology and Information Security teams began to look closely at security and compliance issues in 2009. “We established various security standards and controls based on frameworks such as ISO27001 and sought opportunities to rationalize our security toolsets for better risk management,” he says. Endpoint security was one of the initial areas McGinnis pinpointed. “Endpoint security consisted of several different solutions that didn’t always talk to each other,” he explains. “We wanted to drive down costs while improving our risk posture.”

At about the same time, in early 2009, the disk and endpoint encryption solution Broadridge had deployed was coming to end of life. “Our licenses were expiring and it didn’t integrate with our broader security footprint,” McGinnis says. “We decided that we should look for an endpoint security and encryption solutions that were integrated and would talk to each other.”

McGinnis and his team settled on Symantec Endpoint Protection and PGP Whole Disk Encryption from Symantec. “Symantec had just recently acquired PGP and was in the process of integrating it into the larger security portfolio,” he says. “With Symantec Endpoint Protection, we were able to take various endpoint security functions and roll them into one solution with a consolidated management console and reporting. We gained substantial efficiencies while improving our overall risk posture.”

**Comprehensive endpoint security**

Whereas Broadridge had only used the antivirus and antispyware components in its previous endpoint security solution, McGinnis elected to leverage more of the features in Symantec Endpoint Protection such as network access control, application control, device control, firewall, and intrusion detection and prevention. “Our endpoints are significantly more secure after the deployment of Symantec Endpoint Protection,” McGinnis says. “Application control allows us to block access to certain applications based on the identity of the user. Device control is particularly important as we are able to control USB drives and CD-ROM drives on select machines and for certain identities.”

The benefits of Symantec Endpoint Protection have been substantial. They range from lower cost of ownership for endpoint security, to improved operating efficiency, to reduced risk exposure.

The integration points between Endpoint Protection and PGP Encryption were an important factor in the decision to select both solutions simultaneously. “We were able to address a number of requirements all at the same time,” McGinnis says. “Because we’re a financial services firm and dealing with publicly listed clients, compliance also played a role here. We must adhere to a strict encryption protocols, and we needed a solution that was more user friendly. Rather than remembering multiple user names and passwords, they only need to remember one set.”

**Efficient, effective encryption**

Over a period of approximately six months, Broadridge rolled out several components from PGP Encryption. “The Whole Disk Encryption component has delivered tangible value for us,” McGinnis says. “The IT staff can multitask when encrypting different devices. The ability to encrypt removable devices gives us added protection. The difference between our prior solution and PGP is night and day.”

Broadridge is also leveraging PGP Universal Gateway Email for encrypting email data. “As we communicate with our partners, it is critical that we perform the appropriate ‘handshake’ during the exchange,” McGinnis explains. “This is where encryption plays an important role.”

“[Security] is ingrained in nearly everything that we do.”

– Frank McGinnis, VP, Corporate Information Technology, Broadridge Financial Solutions
For deployment of both Endpoint Protection and PGP Encryption, McGinnis turned to Symantec Partner OnX, which helped in scoping and planning both projects. “The planning phase of any project is always important, and this is when we typically engage an external provider for assistance,” McGinnis says. “If everything is properly scoped and planned, then the implementation is something that you can do with your own resources.”

The Symantec Endpoint Protection deployment took several several weeks, but the PGP Whole Disk Encryption implementation took much longer. “Broadridge is comprised of a large number of companies and numerous systems,” McGinnis explains. “It took about six months for us to get everything completed.”

Archiving, eDiscovery of communications
When Broadridge was divested from ADP, the firm became a publicly traded company on the New York Stock Exchange. “As a publicly traded company, particularly one in the financial services industry, we are governed by various data retention regulations,” McGinnis notes. At about the same time, the company made several acquisitions that increased the need for Microsoft Exchange archiving and eDiscovery—specifically broker-dealer communications exchanges.

In late 2010, Broadridge selected Symantec Enterprise Vault. With the help of consultants from Globanet, the Broadridge’s team rolled the solution out, including the Microsoft Exchange Journaling and Discovery Accelerator features. “We have regulatory and legal requirements to archive some of our Exchange communications,” McGinnis explains. “And when prompted, whether by HR, legal, or other regulatory requirements, we must be able to quickly search and retrieve email that conform to the guidelines of the request.”

Preventing data loss
In late 2011, Broadridge prioritized data loss prevention as a top priority. “Customer data is sacred to us and maintaining customer confidence is pivotal,” McGinnis says. “We’ve seen an explosion in the amount of data being stored and managed. The business determined that we needed to have a formal program in place to do everything from discover its location, to

Mobile devices and applications are springing up all over the place.”

— Frank McGinnis, VP, Corporate Information Technology, Broadridge Financial Solutions

Encryption implementation took much longer. “Broadridge is comprised of a large number of companies and numerous systems,” McGinnis explains. “It took about six months for us to get everything completed.”

Intelligent messaging security in the cloud
With the endpoint security and encryption projects completed, McGinnis turned his attention to replacing an existing standalone messaging security solution in 2010. “We wanted to align ourselves with a technology provider that was focused much more broadly than email delivery, a security provider versus a delivery provider,” he says. “We sought a global perspective and a provider that was looking at potential outbreaks elsewhere that could impact our environment and help us to proactively avoid problems before they happen.”

Broadridge looked at various hosted solutions and ultimately selected Symantec Email Security.cloud. The fact that all incoming content is checked and filtered in the cloud before it gets to Broadridge’s environment is important for McGinnis. “It integrates seamlessly into our environment,” he reports. “We have multiple checkpoints, a number of which rely on Symantec solutions, such as Symantec Endpoint Protection’s network intrusion detection and prevention. We take a holistic approach to security, and messaging security is one of them. We saw Symantec Email Security.cloud as an important building block.”

With the deployment of Symantec Email Security.cloud, McGinnis’ team experienced a dramatic drop in the amount of spam getting through the network. This drove productivity gains for end users. “The ability to adjust our filtering policies and the expanded categorization gave us much greater flexibility in configuring the solution to what was transpiring in the threat landscape and our business requirements,” McGinnis reports. “Our prior solution was a one-size-fits-all approach; with Symantec.cloud, we can create policies for groups and even individuals. This further reduces the amount of spam and false positives. The payload-based encryption capability is another feature we’ve found quite useful. We can send a link internally or externally, ask them to click on it to validate their identity.”
monitor it—both in motion and at rest—and to manage and control it. It became a risk that the business felt needed to be addressed.”

McGinnis’ team and the Broadridge Information Security team began with a proof of concept in early 2012. “We looked at a couple of different data loss prevention solutions, which included Symantec’s,” he says. There were three primary factors that favored Symantec Data Loss Prevention. The first was the ability to monitor and manage information at the endpoint. “We wanted to look at information not only at the network but at the endpoint,” McGinnis states. “We sought to control it where it starts rather than after it is already in motion.” The second reason was data loss prevention that spanned multiple sources—storage, the network, and endpoints—and provided integration with existing security solutions. The third was the need for a solution that would evolve with changing business requirements. “The threat landscape gets harder and harder to address,” McGinnis says. “We sought a solution that would evolve with it.”

With a decision in place on the technology component, Broadridge Security Engineering worked with the business, which included representatives from HR, legal, and business units, to identify and define data loss prevention policies. The built-in policies in data loss prevention provided a solid foundation. “We began with security standards such as ISO27001 and other compliance programs that we follow,” McGinnis says. “We are now expanding beyond those to address specific business requirements.” The Broadridge team is scheduled to complete the entire implementation by the end of 2012.

Now that Broadridge is able to monitor and control critical aspects of its data, McGinnis is preparing for the next step. “We want to understand who created the data, who is using it, what retention policies are tied to it,” he observes. With that in mind, Broadridge is looking at several different technology options for doing so, including Symantec Data Insight.

A whole new mobile world
Mobility is the latest initiative that McGinnis is working to tackle. “Mobile devices and applications are springing up all over the place,” he says. “The potential is not simply on the consumer
front but for the business as well.” Broadridge began allowing corporate-owned mobile devices a couple years ago, and McGinnis and his team extended controls and processes for managing them. They have looked at the possibility of permitting employee-owned devices but are still in the process of formulating a corporate strategy.

Mobile is really much broader in scope than the device and the app according to McGinnis. “It could be any number of devices that are accessing information via a wireless network,” he says. “This is an important recognition that many IT organizations fail to acknowledge when building out a mobile computing or BYOD program.”

For the mobile devices at Broadridge, McGinnis’ team rolled out Symantec Mobile Management in 2011. “It helps us address issues such as how do we provision apps to the devices, wipe them when they are lost, institute audit policies and reporting, and manage corporate data policies,” he explains. “As we figure out our mobile computing approach, we plan to look at Symantec App Center as a means for creating virtual containers on personal devices that can separate personal and corporate data.”

Ironically, mobility is even changing the traditional IT roles at Broadridge. “What was your typical LAN administrator a few years ago is not your typical LAN administrator today,” McGinnis points out. “Endpoint computing is broader than a set of desktops and laptops. The function must now address mobile devices and apps as an example. An associate may have a tablet, smartphone, laptop, and maybe even a desktop.”

To protect the data accessed and retrieved on the mobile devices, Broadridge plans to add Symantec Data Loss Prevention for tablets later this year. “The data accessed on the devices, whether BlackBerry or Apple smartphones, is immensely more valuable than the devices themselves,” he observes. “With Symantec Data Loss Prevention, we are able to do everything from monitor the information accessed on each device to enforce different policies such as encryption for data in motion, including encrypting email when users are sending data.”

We take our stewardship of IT systems and corporate information very seriously.

— Frank McGinnis, VP, Corporate Information Technology, Broadridge Financial Solutions

A failure to protect Broadridge’s systems and information could have extensive repercussions. A few minutes of downtime due to a malware intrusion could interrupt and delay hundreds of thousands of customer transactions. A breach of one database or exposure of a handful of records could reveal highly confidential customer information.

A longstanding—and longsuffering (as the Jets haven’t played in a National Football League Super Bowl game since 1968)—New York Jets fan, McGinnis likens a strategic security and compliance program to an All-Pro offensive line. “Given the right levels of protection, a quarterback can pick a defense apart,” he relates. “And while the offensive line doesn’t actually run or catch the winning score, it does enable the larger offense to score. Without it, an offensive unit is often futile—or at the best ineffective.”

The same is true of a security and compliance program that assumes a proactive threat management approach. “We take our stewardship of IT systems and corporate information very seriously,” McGinnis asserts. “Security can be a critical business enabler, helping the larger business to succeed. But if it isn’t effective and falters, business operations are interrupted and customer information is put at risk.”

Put all of the security and compliance pieces together, and you have an IT organization that is poised to become an offensive juggernaut.

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest.

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest.

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest.