

NONPROFIT STRENGTHENS ITS SECURITY INFRASTRUCTURE

The National Restaurant Association's FireEye and QRadar rollout bolsters network security, says CIO Ed Beck.

As advanced persistent threats continue to wreak havoc on networks, the National Restaurant Association deploys a top-tier solution to guard against attacks.

At a Glance

ORGANIZATION: National Restaurant Association

LOCATIONS: Chicago and Washington, D.C.

NUMBER OF EMPLOYEES: 250

FULL-TIME IT STAFF: 34

SUMMARY: Established in 1919, the National Restaurant Association is the largest food service trade association in the world (by membership), supporting nearly 500,000 restaurants. It develops tools and systems that help members train employees and increase revenues and profitability. It also advocates for favorable legislation and regulations, and provides networking and research resources and food safety education and certification programs.

The National Restaurant Association has never been willing to rest on its laurels. That's one reason why the nonprofit organization has thrived for nearly a century as the leading voice and advocate for America's hundreds of thousands of eateries.

It's also why the association is the No. 1 provider of food safety education to the food service industry through its ServSafe Food Safety Training Program, which has certified more than 4 million food service professionals through its Food Protection Manager Certification Exam. While there are still some customers who complete their coursework and exams through the mail, most interaction now takes place online. Activity on the organization's e-learning platform has been growing by 9 percent annually. In 2014, nearly 1 million students used the online system.

So when CIO Ed Beck decided it was time for the National Restaurant Association to take its IT security to the next level, he won immediate support from the organization's top executives.

"Everything we do with technology is wrapped around our business and better serving our customers," Beck says, noting that the organization handles (but does not store) credit card numbers, personal identifying information and confidential member data. "How do we ensure a consistent flow of customers to our websites? We do that by ensuring that people and the businesses they work for feel safe interacting with us, and we're always going to do everything we can to give them that peace of mind."

The National Restaurant Association has long met the industry standards for network security, but Beck became alarmed by recent attacks on major retailers. He decided that the increasingly aggressive threat environment required that his organization proactively upgrade to a security solution that is based on the framework set by the National Institute of Standards and Technology.

"Ultimately, we were looking for a way to better defend against advanced persistent threats [APTs]," Beck says. "Beyond viruses and malware, these are things that can compromise and take down a network."

Beck and his IT team turned to CDW for assistance and decided to make a significant investment in a top-tier, enterprise-grade solution that included three FireEye NX4000 security appliances and the IBM QRadar security and information event management (SIEM) system.

Setting a Foundation

When Beck took the helm of the IT team at the National Restaurant Association in 2012, upgrading security topped his to-do list. Before he could move forward, though, he needed to bolster the organization's underlying IT infrastructure.

Around that time, the National Restaurant Association established a close partnership with CDW. "The thing I value most about CDW is that they're always looking at things from a holistic point of view, which means that they're looking first at helping me find the right solution for my needs," Beck says. "They're less worried about what product I select than whether or not it's going to work with the rest of my environment and deliver the results that I need."

With its deep resources in networking, security, storage and telephony, CDW brought a wealth of insight to the project, says Patrick Echols, nonprofit account manager for CDW.

"We also have relationships with partners like Cisco, Microsoft and FireEye, so if there's ever a question that we can't answer, we can pick up the phone and say, 'Look, this is what's going on: How can you help us?'" Echols explains. "That ability to get answers and provide whatever assistance is needed is something that is of real value to our customers."

The National Restaurant Association's first step in retooling the IT environment was to work with CDW to set up a new colocation facility to bolster its disaster recovery capabilities. They then upgraded the association's networks in Chicago and Washington, D.C., to the Cisco Unified Communications System, adding UCS blade



\$76.9 billion

The amount organizations are expected to spend worldwide on information security technology and services in 2015, an increase of more than 8 percent from 2014

SOURCE: Gartner, "Forecast: Information Security, Worldwide 2012–2018, 2Q14 Update," August 2014

servers, Check Point firewalls, Cisco Catalyst switches, Nimble storage and additional bandwidth in order to better serve the growing number of online customers.

Moving Ahead

In early 2014, Beck and his team began researching their options for a beefed-up security solution. Their requirements were specific: Not only did the tools need to detect, locate, manage and secure APTs, but they also had to be compatible with VMware and relatively easy to use.

After discussing his vision with CDW, Beck chose what he considered to be a strong one-two punch: FireEye and IBM QRadar. The FireEye Network Detection System is a game changer in network security because it prevents, detects and responds to network-based, zero-day exploit attempts. It also defends against web drive-by downloads and advanced malware attacks.

These types of attacks are dangerous because they can easily and silently bypass conventional defenses, which detect threats only by their signature. By contrast, FireEye relies on routinely updated virtual data analyses to identify and block new types of malicious threats — the first time it detects any abnormal code or process.

"FireEye is as close as you can get to removing all doubt that you're fully protected, from a malware perspective, because it's beyond firewalls and all the conventional defenses most people usually have," says CDW Security Specialist Chad Morris. "It's really the industry standard today."

The QRadar SIEM system complements FireEye by providing Beck and his team with real-time visibility into log data from servers, firewalls and other components, and includes alerting capabilities. "QRadar allows us to quickly respond if FireEye finds a problem, and it also helps us improve our ability to shift and adjust performance," says Beck, noting that he chose QRadar from several leading products because its interface works well in a VMware environment.

Morris characterizes the new security solution as "forward thinking" and "full-bore."

"The two products together provide them with a far more effective threat management capability because they can see everything for all different egresses, from all aspects of their environment," he explains. "Each magnifies the value of the other."

Last summer, the National Restaurant Association installed a FireEye NX4400 appliance at each office and at the colocation facility, or as Beck describes it, "each point of the perimeter."

Prepare to Succeed

Investing in top-tier security appliances and log management software is a great first step, but it's not enough, says National Restaurant Association CIO Ed Beck. Organizations also have to be well positioned to manage risk and respond quickly in the event of a security breach.

The National Restaurant Association took the following steps to further safeguard its IT environment:

- **Prioritized security:** A lot of people view security as an aspect of networking, but not Beck. "The more I've been involved in putting in component pieces to improve our security, the more I've seen that it needs to stand alone, that it needs to be viewed as a self-sustained holistic environment, not an add-on," he says.
- **Created a new position:** To make sure security maintains its singular status, Beck created a new position — director of information security and risk — that reports directly to the CIO and whose "sole responsibility is security," Beck says.
- **Prepared for problems:** The IT team consulted with the organization's general counsel to establish a security review process for all systems and components and to design and publish a detailed incident response plan. "When things go wrong, you need to have a process in place so that people can become involved and not waste valuable time figuring out what to do," Beck says.



23

The number of zero-day vulnerabilities discovered in 2013, a 61 percent increase over 2012

SOURCE: Symantec, "Internet Security Threat Report: Volume 19," April 2014

Gaining Business Benefits

CDW assisted the IT team in implementing both products, an effort that went off without any complications. "CDW was amazing," Beck says.

The FireEye appliances were almost plug and play, but the QRadar system involved a steeper learning curve, "mainly because there's so much data now being collected," Beck notes. "CDW helped us understand how to set it up and customize it and then how to move forward with it."

"Obviously the recently well-publicized IT security issues throughout industry were of great concern to us," says Marvin Irby, the association's chief administrative and financial officer. "Our members and customers expect that their information is managed with the highest degree of integrity. I was pleased with the proactive approach proposed by the CDW team to enhance our capabilities in that area."

Since putting the new solution in place, the National Restaurant Association has enjoyed a marked reduction in risk, while gaining a unique understanding of how truly pervasive security threats are in today's environment.

"You can't fight what you don't know, and hidden threats are, in my opinion, the single largest threat to everyone," Beck says. "But from the moment we installed this solution, it began to highlight more than just the threats we need to react to — it also helped us to proactively seek out and go after potential threats."

The new capability also helps the IT team train its employees and customers about the risks inherent in working online. Beck cites an example: Employees see and decide to click on an ad promising a free cup of coffee; the ad probably is a phish, but it could also contain an APT.

"The moment they click on it, the system automatically alerts us and quarantines their system," Beck explains.

"Now, we can go in and talk to them: 'Look at what could have happened if FireEye had not caught this.' So hopefully, they'll learn from that and modify their behavior in the future."

The association's decision to invest in a top-tier security solution is already providing clear returns. An enhanced security solution also acts as a differentiator in the marketplace. Although the National Restaurant Association is a high-profile nonprofit organization, it still competes with other associations and food safety certification firms for membership and customers.

Security is fast becoming a top criterion for every major service and retail business employing the National Restaurant Association's services, says Beck, who also notes that one firm recently required his IT team to fill out a 10-page questionnaire on the organization's security posture.

"More and more, if your partners and customers want to know about your total security level, and if you're not where they think you should be, they do not want their employees on your system and they don't want to be interacting with you," Beck says. "They're not only looking for a product that gives them the best value but also the least risk."

With its new security solution now in place, the National Restaurant Association can assuage any concerns its members and potential customers may have. "We can say to a very large customer, 'Not only are we PCI secure, but we went above and beyond that to put in place a top-tier security solution and processes,' and then talk about what we do and how we do it," Beck explains. "This helps them see the value we bring to the table from a security standpoint."



Check out CDW's infographic on next-gen security at cdw.com/NextGenInfographic.

Jonathan Timmes



TWEET THIS!

This content is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW-G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.

All other trademarks and registered trademarks are the sole property of their respective owners.

Together we strive for perfection. ISO 9001:2000 certified

144903 – 140822 ©2015 CDW LLC

