The Company
As one of the largest public retirement services providers in the nation this organization currently manages the retirement accounts of approximately 272,000 educators, and provides benefits in excess of $2.2 billion per year to approximately 75,000 retired individuals and their families.
In executing those duties, the organization is required to maintain detailed profiles of its members, including the individuals’ most sensitive personally identifiable information -- from their names, addresses and social security numbers to their confidential healthcare records.
The organization’s Chief Security Engineer is charged with ensuring that the organization’s IT systems and network infrastructure are protected from external attack and internal abuse. In addition to maintaining compliance with the agency’s own rigorous data security policies, he must also prepare the business for regular external audits and yearly accreditation reviews based on federal guidelines for the protection of financial, health care and personal information.

Solution Summary

<table>
<thead>
<tr>
<th>CUSTOMER TYPE</th>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public retirement services provider.</td>
<td>Finding a professional-grade security testing product that goes beyond open-source tools and point product reporting capabilities to validate IT systems defenses and the protection of electronic data.</td>
<td>CORE Impact® Pro, the first comprehensive penetration testing software solution for assessing organizations’ most significant IT vulnerabilities and information security threats.</td>
</tr>
</tbody>
</table>

“The Challenge
The organization needed an integrated set of security testing tools to emulate cutting-edge hacking and malware exploitation techniques and ensure that its systems and end users could not be subverted by attackers seeking to break into its stores of sensitive information.

To meet the requirements of its internal compliance teams and mandated third-party security auditors, the company sought a professionally developed testing package that would level sophisticated exploits at its IT systems and generate detailed security status reports that could be shared with both internal management and external assessors.

As part of its project, the business also aimed to surpass the efforts of other organizations facing regulation from the same constituencies to prove that it is maintaining an above-average stance in terms of defending the personally identifiable information of its members.

“If you can, you always want to try to do more than the next organization, because you know that these teams of assessors are looking at what you do and comparing that to other groups in terms of best practices,” said the Chief Security Engineer. “Our primary goal is to protect our members’ data, but we also want to make sure that we are perceived as going beyond the status quo to do so.”

The Solution
To extend beyond its previous practice of using open-source freeware and limited penetration testing features built into its network security systems to validate the efficacy of its defenses, the organization licensed CORE Impact Pro and began conducting regular reviews of its networks, endpoints, applications and end users to ensure that it is not vulnerable to attacks and subsequent data theft.

In addition to testing the effectiveness of its perimeter defenses, including its firewalls, anti-virus applications and intrusion detection systems, the organization has also used CORE Impact to validate the usefulness of its internal security policies, such as the ability of its staff to respond to emerging attacks.
Based on the ease-of-use and level of automation offered by the package -- specifically in comparison to open-source penetration testing tools that forced the company’s IT department to engage in the time-consuming work of scripting exploits -- the organization has begun launching weekly assessments to ensure that it is protected from the latest software vulnerabilities and attacks.

The retirement benefits provider has also begun using Impact Pro to prepare for mandated external audits of its overall security posture to ensure that it does not face fines or added scrutiny from government regulators.

“To prove that our security testing is both consistent and unbiased, we’re required to have an outside entity provide us with accreditation. Because of the approach we’ve established testing with CORE Impact, and the ability to respond quickly and patch any issues, we remain confident that auditors will recognize that we’ve tested everything to best of our abilities in the same manner that a hacker would,” the Chief Security Engineer said.

“One of the most valuable aspects of using Impact is the ability to show that our IDS, antivirus and firewall systems are working correctly, it lets us know that we are doing the right things in terms of securing our assets, and doing them well. This gives management a good feeling about the money we’ve already spent, and it becomes easier to get confirmation for the necessary renewals, especially when we pass all the various audits we face.”

The Result

Giving staff more time to execute tests

Rather than involving itself in the time-consuming manual exploit scripting demanded by open-source penetration testing frameworks, the organization’s staff is using the out-of-box exploits offered in CORE Impact to save work hours and expend more of its energy carrying out security auditing tasks themselves.

In utilizing CORE Impact’s onboard exploit code, and the software’s ability for testers to write their own scripts if they so choose, the company contends that it is able to assail its systems with the latest in malware attack techniques.

“With the open-source tools it was always hit and miss based on how frequently the community supporting the technology was updating its exploits,” said the Chief Security Engineer. “We found in some cases with those tools that the materials involved were years old and out of date. With Impact we know we’re getting the latest and greatest in terms of what real hackers can throw at our defenses.”

Standing up to external audits

The company is required to undergo regular audits from both state and third party security assessors that address both its ability to protect members’ confidential financial data, and its compliance with requirements to safeguard healthcare records that were modeled on the federal government’s Health Insurance Portability and Accountability Act (HIPPA).

In addition to passing those audits with greater ease since installing CORE Impact, officials with the organization contend that assessors have recognized that the organization is going above and beyond the efforts of other groups that are required to submit their operations to similar scrutiny.

“Impact allows me to validate all our work and ensure that we are going to face audits with the best possible approach to securing our systems,” the Chief Security Engineer said. “And based on the fact that a lot of other agencies aren’t using it yet, that really puts us in a good light with auditors. We tell them we’re using this technology and they immediately understand that we’re being vigilant.”

Validating budget, investments and ongoing projects

Since licensing CORE Impact Pro, it has become far easier to defend spending on new and existing security technologies and initiatives as the application of more comprehensive security testing has given the organization the ability to prove which of its defense mechanisms are working, and where it needs to make additional investments.

The Chief Security Engineer said that Impact Pro also helps non-technical constituencies understand his group’s work, and the challenges it faces in keeping the organization safe from the rapidly expanding range of attacks emanating from the hacking and malware communities.

“We’ve often struggled from the perspective of expressing everything that we do in the role of network security engineers. People sometimes look at this work as voodoo,” he said. “Using Impact helps us explain, illustrate and validate what we do and how we have to think just like a hacker would to do our jobs right.”