

Sierra Pacific Mortgage protects its customers' sensitive financial information with the help of a Quest vCISO

JIM CONNELL, CHIEF INFORMATION OFFICER OF SIERRA PACIFIC MORTGAGE, says changes in his industry and escalating online threats make it mission-critical that his organization employ a vCISO to handle its cybersecurity.

A vCISO (often pronounced “v-SEE-so”), is a virtual Chief Information Security Officer, and has become an important position in the cybersecurity industry.

As Sierra Pacific's vCISO, Quest's Joe Hagerty takes a C-suite-level responsibility for the organization's entire security position. As the word “virtual” in the title implies, he is able to do so while saving Sierra Pacific the sizable expense of [hiring an in-house CISO](#). While working as an employee of Quest, Hagerty is able to help Connell deliver fortified IT security thanks to an agreement in which he devotes two days a week to Sierra Pacific and essentially provides 24/7 emergency availability.

Connell says Sierra Pacific needs a partner with executive security experience partly because of increasingly strict governmental oversight. In the wake of the 2008 mortgage crisis that helped trigger the Great Recession, new federal and state regulations changed fundamental elements of his company's workflow. In today's mortgage industry, there

are countless reports that need to be sent to various agencies, numerous Internet audits, and — most importantly — tightened security requirements.

Cybersecurity now sits at the core of Sierra Pacific's essential business. Because his company manages hundreds of millions of dollars and has detailed

financial information about tens of thousands of individuals, it is a prime target for cyber criminals. “And over the past decade, as we all know, cyber crime has exploded,” Connell says.



Jim Connell, Chief Information Officer, Sierra Pacific Mortgage

Connell, who has been an IT director and senior project manager for more than two decades, witnessed the evolution of cyber criminals first hand. “First there were the ‘hackers’—vandals who just enjoyed breaking into networks,” he says. “Then the solo criminals showed up, and then teams in garages. Now there are state actors — nations funding institutions that work out of office buildings filled with experts in specific roles.”

“Obviously if something goes bad with your IT security, that's a red-alert emergency,” Connell says. “We recognized early on that we did not have the skill sets or tools to tackle that challenge. That's why we formed our partnership with Quest.”

Quest helped Sierra Pacific build an [in-depth security model](#) with layers of defenses, including multiple firewalls. Quest installed protections such as multi-factor authentication throughout the operation and helped the entire team develop defensive protocols.

All of this paid off in 2017, Connell says, when the security team discovered that bad actors had broken into Sierra Pacific's email server and had begun forwarding emails to offshore accounts.

“Joe and the Quest team were able to stop the attack quickly and remediate the issue without any financial losses to any of our customers,” Connell says.

To ensure that consumers are protected from such attacks, the 49 states where Sierra Pacific operates each have their own set of security auditing and reporting requirements, which Quest helps the organization navigate.

“We are not just checking boxes” Connell says. “We are being prudent by protecting our business and our customers. And it's important to us that our partners have top-down integrity.”

“Obviously if something goes bad with your IT security, that's a red-alert emergency. We recognized early on that we did not have the skill sets or tools to tackle that challenge. That's why we formed our partnership with Quest.”

Does your organization need a virtual CISO?



TIM BURKE | President and CEO

CYBERSECURITY HAS BECOME A CORE CONCERN IN RECENT YEARS FOR ANY ORGANIZATION THAT DEALS WITH SENSITIVE INFORMATION.

With large-scale cyber attacks in the news practically every month, more and more companies have determined that they require the services of a highly experienced security expert — the Chief Information Security Officer (CISO). These are folks with enterprise-level experience who, as officers of the company, make certain that security is embedded in the organization's mission and day-to-day operations.

As demand for CISO services has exploded and CISOs have become more valuable, they've become very expensive to hire. As a result, many organizations choose to work with a security company that employs what is known as a virtual Chief Information Security Officer, or vCISO. If you are wondering whether or [when to hire a virtual CISO](#), here are a number of good reasons to choose that route.

Inviting a vCISO into your C-suite allows you to leverage the expertise that person has developed over a career as a security expert. In many cases, the vCISO will work with your existing security team, either in a scheduled part-time arrangement or on an on-demand basis. While technically [employed by the technology management or security firm](#), they might report to your CEO, CIO or board of directors. Some companies will only need a vCISO's services for four or five hours a month, while others might require a part-time position. This might entail a monthly or annual contract.

It is the nature of a vCISO to take absolute personal responsibility for your organization's cybersecurity. This usually means putting in place a comprehensive set of policies, procedures, technologies, and controls.

In many circumstances, working with a vCISO under a [Professional Services agreement](#) can be smarter and safer than incurring the much greater expense associated with building an in-house security team.

Because they work for many organizations in a variety of industries, a vCISO probably has more experience than his or her colleagues working full time for one company. Most individuals rarely have to deal with a critical security breach, whereas a vCISO might handle an incident response situation once a week.

Because the vCISO position has been virtual since the job title was first coined, they are adept at working with clients all around the country. That means when you look to hire for a vCISO position you're not limited to local candidates.

Your vCISO often serves as compliance officer when it comes to dealing with regulators. They also can be responsible for creating quarterly or annual reports for regulatory agencies and boards of directors. Because a person with CISO training and credentials is recognized as an expert in the security field, these reports have extra weight and, frankly, more credibility.

There's another thing I'd invite you to keep in mind when deciding whom to entrust with your organization's cybersecurity: the best vCISOs work for a company that is staffed by a team of cybersecurity experts. Your contract will be with that company, and you should have virtual access to all of its resources, including up-to-date security technologies and an experienced Incident Response Team.



I hope you found this information helpful. As always, [contact us](#) any time about your technology needs.

Quest © 2021, and How can we help?® are registered trademarks of Quest Media & Supplies, Inc.