SecurityScorecard

CASE STUDY

Software-as-a-Service Company, Providing Cloud-based Human Resource Solutions, highlights multiple benefits from use of SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

THE CLIENT

This cloud-based human resources (HR) solutions provider enables small and medium-sized organizations (SMB) to focus on their core business without needing to have their own internal HR department. The company has 100,000+ users, 10,000+ clients, and a lean security team. Because it performs the overwhelming majority of its services in the cloud, securing the data for this Software-as-a-Service (SaaS) company is a priority.

The company offers SMBs an array of employee and employer services including: payroll processing, human capital consulting, employment law compliance, and employee benefits, such as health insurance, retirement plans, and workers compensation insurance.

The company also performs the back end work for reporting employer taxes to the Federal government. In 2014, the company processed over $25 billion in payroll and payroll tax payments. In that same year, the company became a publicly- traded organization.

THE CHALLENGE

The attack surface of organizations has widened in the last several years. The use of more cloud-based solutions, an increase in connected devices and employee-owned devices has increased the number of access points an organization has. Information security professionals are generally quite aware of the strengths and weaknesses of their own security programs. When it comes to partners, vendors, and suppliers, however, most organizations struggle to have visibility and awareness into the accurate risk of their third party ecosystem.

Attackers often target third parties with a larger organization as a primary target to pilfer a treasure trove of customer and employee data, sensitive financial information, and intellectual property. Smaller third parties don't often have the resources to properly secure their networks and hackers take advantage of that. Security teams are trying very hard to keep pace with attacks that may target any new technologies being attached to their company's infrastructure via cloud systems signed. In order to stay nimble, the client's business departments, who have identified a need for a solution or technology, want to ramp up quickly without IT or security review and approval, increasing the risk of a breach.

"Security takes a Herculean effort to keep an eye on everything. There are so many things being done behind the scenes to constantly test, hack, and probe our own systems by my team. One of the most challenging areas of our jobs, however, is understanding the risk brought to us by our partners and vendors, many that we have never interacted with, until recently."

THE CHALLENGE

There is also this mantra from executives that the Director of Information Security needs to keep in mind: “Keep us out of the news.”

It is a message all security teams have heard before. Unfortunately, more and more organizations are struggling to avoid being embarrassed by a data breach. Breaches are bad for business. Stockholders hate them. Customers feel exposed. They damage reputations, brands and are very costly for an organization to respond to. For the leaders of security teams, breaches shine a big, bright spotlight on security investments and measures. Executives want to know why they have invested so heavily in security, yet cannot keep attackers away from sensitive data.

“The current methods for collecting third party risk information are inadequate and deficient”, relayed the Director of Information Security. “No company wants to transparently expose its security and risk posture to others, despite the advantage companies have by working together and sharing intelligence to allow their systems to communicate with each other”.

The Director of Information Security explained that the reports used to perform diligence on vendors and partners, such as Service Organization Control (SOC) reports and pen and paper questionnaires, are not providing enough security detail in the context of its interaction with a company’s systems. “These reports have questions on very basic information and controls, such as backups, physical security assets, locations of data centers, network and firewall information, but they are an overview at best, and don’t provide specific enough insights”.

“You can also pay for really elegant reports from penetration testing efforts and present them to your management team,” said the Director of Information Security. “Penetration testing has its place in security, but it is only a single point in time [assessment]. What happens when a configuration changes a few weeks after the testing and reporting has been presented? The threats we are seeing now are a lot more dynamic than any single test can possibly capture.”

THE SOLUTION

The company uses SecurityScorecard's rapid, accurate security rating platform to gain immediate visibility into the risks lurking in third party environments. Whether it is the patching cadence of partners, their Endpoint Security Score, the number of malware infections, or the number of company mentions on hacker chatter forums, SecurityScorecard grades the company's partners across the entire security landscape. The SecurityScorecard platform allows the Director of Information Security to see exactly where that partner stands, at the moment they need to know that information.

"The first thing I do when a new vendor or partner is going to be onboarded is pull up the SecurityScorecard dashboard, type in the url, and we have a quick, accurate assessment," said the Director of Information Security. "The SecurityScorecard platform is brilliant. To have the knowledge that we cannot get in a questionnaire or a SOC report about a third party is a force multiplier for us... We can do more security review with less resources."

The Director of Information Security takes the information and uses it to dig deeper into the 10 security factors from the SecurityScorecard platform, and begins their conversation with that partner to validate and fix any issues that would put the company, or their partners, at risk.

> "The first thing I do when a new vendor or partner is going to be onboarded is pull up the SecurityScorecard dashboard, type in the url, and we have a quick, accurate assessment."

- The Director of Information Security

THE RESULTS

The company now has a more direct way to measure its own security maturity against its vendors and partners—and executives have a window into security risk in a context they can understand. The company can better gauge and track real world security risk with all the partners it depends on to perform its business optimally.

Since the SecurityScorecard platform is continuously monitoring vendors and partners of the company, the Director of Information Security can then establish a historical mapping of the security posture over time, and use that in their reporting to management. The Director of Information Security also uses information gleaned from the platform in security steering committees to better educate and communicate larger risk trends in security.

- **Another benefit SecurityScorecard provides the company is the flexibility it needs as a cloud-based SaaS provider.** *"How can we remain a nimble enough organization to enable business units with clear, security caveats?" observed the Director of Information Security. "We cannot be in the business of saying 'no', so a solution like SecurityScorecard allows us, for example, to better obtain some control on cloud and SaaS implementations, or better understand complicated Single-Sign On (SSO) authentication issues of a partner. We also use SecurityScorecard to evaluate and benchmark ourselves and measure our own maturity."*

- **The alerting capabilities of the platform are another well regarded feature of the platform. When the Director of Information Security receives an alert, they immediately reach out to their network operations team, then look at the vulnerability console to check whichever security factor triggered the alert within SecurityScorecard.** *"I am happy to get alerts," the Director of Information Security noted. "Most of us do not know exactly when there is a breach, so our reaction time is very important. The platform allows us to find gaps and exposures quickly, and accurately. Before having this, we were wearing blinders."*

ABOUT SECURITYSCORECARD

Funded by world-class investors including Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, and cyber insurance underwriting. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating.

FOR MORE INFORMATION, VISIT SECURITYSCORECARD.COM OR CONNECT WITH US ON LINKEDIN.

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
New York, NY 10017
1.800.682.1707

SecurityScorecard