SecurityScorecard

Children's MINNESOTA

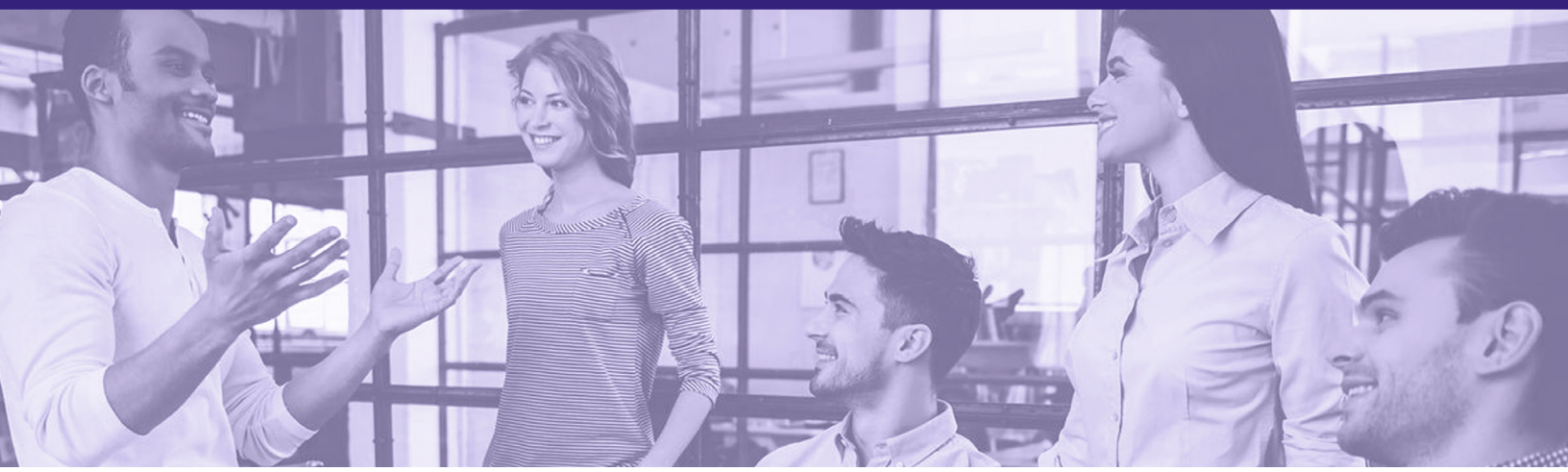
CASE STUDY

Children's Minnesota

SecurityScorecard.com
info@securityscorecard.com

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

ABOUT THE **CLIENT**



Children's Hospital of Minnesota is one of the largest independent pediatric health systems in the United States, with two hospitals, twelve primary care clinics, six rehabilitation and nine specialty care sites. As a healthcare nonprofit, Children's Minnesota is subject to HIPAA regulations and must ensure that personal health information (PHI) is secured, both at physical locations and within electronic health records and exchanges.

We spoke to Chief Information Security Officer Paul Hypki. Hypki has over 13 years of experience with risk management. His responsibilities at Children's Minnesota include creating and implementing information security policy and promoting risk remediation within the organization.

THE **CHALLENGE** OF ENTERING **A NEW LANDSCAPE**

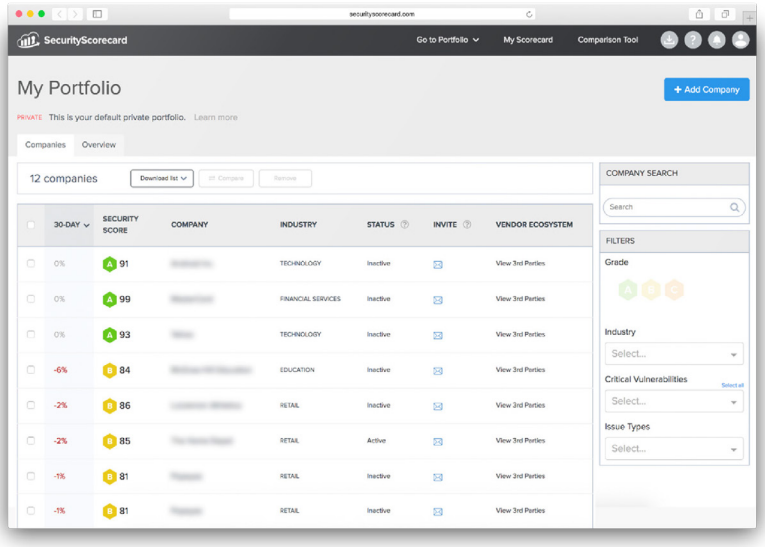
According to Hypki, one of the challenges for CISOs when new to a hospital system is selecting a security benchmark and policy that is meaningful and then sourcing the information to measure against that benchmark.

Hypki says, “When I started, I could have compared our cybersecurity performance with my old employer’s, but Children’s Minnesota would prefer that we adopt a security profile that mirrors well-known Children’s hospital systems in Boston, Seattle, and/or Colorado.” While Hypki was equipped with the understanding of how to create a benchmark, the next obstacle was where to find and how to present information on these hospital systems with similar security challenges and performance benchmarks. It’s at this juncture that Children’s Minnesota began to leverage the SecurityScorecard platform to gain visibility into potential security risks–internally and externally.

THE EXECUTIVE'S OVERVIEW–**EVALUATING PROGRESS** AGAINST THE BENCHMARK

Immediately, Hypki was able to pull information on hospital systems in Boston, Seattle, Texas, and Colorado and see how their scores compared to Children's Minnesota in one comprehensive view.

This allowed Hypki to show the executive team how Children's Minnesota's risk profile compared to other healthcare systems. It also gave him the ability to quickly conduct cross-industry comparisons by selecting local, well-known healthcare organizations and discover how Children's Minnesota scores lined up with this portfolio. As a result, the platform armed him with the information to communicate how to define organizational risk tolerance and where to focus efforts on improving cybersecurity health.



Hypki has used the breadth and depth of findings surfaced by the SecurityScorecard platform to show that there are risks that must be quantified and considered in determining what level of risk is acceptable. Providing this sort of education and visibility on risk management at the board level is one of the contributing factors that has allowed Hypki's team to improve the cybersecurity health of Children's Minnesota- progress that Hypki is able to easily quantify and report on.

While Hypki provides these reports to management on a quarterly basis, his team actively interacts with the tool on a weekly or even daily basis to monitor and remediate risk factors on a real-time basis.

MAKING PROGRESS AGAINST THE BENCHMARK-

IMPROVING CYBERSECURITY HEALTH

From a day-to-day perspective, the risk management team's goal is to remediate risk and, consequently, improve the score of Children's Minnesota with each quarterly report to management. "My team is looking at the information from a risk management perspective. They are easily able to scroll down into the finding to identify what issues are most critical for us," he says.

This allows Hypki's risk management team and Security Operations Center (SOC) to review and prioritize security issues and communicate these priorities to the IT team at Children's Minnesota. Hypki attributes the success in improving Children's score over the past months to developing a collaborative approach with the IT department where they set expectations, set a process to escalate issues with the IT team's ticketing workflow, and most importantly, set priorities in a way that addresses key risk factors. For the Children's Minnesota risk management team, this means using the priority level of each risk factor and issues surfaced in the platform in combination with their understanding of the potential impact to the institution to set a priority that is risk-based, reflective, and that empowers risk-based remediation.

"The magic here is that this is really a tool that helps to identify a risk that we might not be aware of. Plus, this tool is really allowing us to drill down ...to the point where I can tell you which machine is causing a lower patching score."

EVALUATING RISK

Evaluating Ecosystem Risk

Hypki also uses the platform to gain visibility into the potential risk posed by Children's Minnesota's critical vendors. Occasionally the findings simply provide a level of secondary validation or comfort regarding a firm's security–for instance, the company's security consulting firm having a good score. Other times, Hypki uses the data surfaced by the ten risk factors to actively monitor vendors that store or access sensitive data, such as a data center vendor.

Of special appeal are the collaborative features of the tool that allow him to share information with a critical vendor, which results in remediation and reduced risk to Children's Minnesota. "What we are trying to do is reach out to our key third party vendors and help them be more secure- because that also helps us," says Hypki.

Evaluating the Risk of Potential Partners and Acquisitions

Beyond looking at the risk within the current ecosystem Hypki also considers the potential risk encountered when that ecosystem might change. When Children's Minnesota is considering partnering with or acquiring another company, Hypki looks at their scorecards to gauge potential risks for these companies.

A LOOK TO THE **FUTURE–COMPLIANCE** AND BUILDING **THE EVIDENTIARY LOG**

An upcoming initiative for Children's Minnesota is to align their benchmarks and security policy with the NIST Cybersecurity Framework, Hypki anticipates being able to leverage the Compliance function of the SecurityScorecard platform to clearly see which issues map to specific NIST controls. Additionally, Hypki envisions pulling screenshots and historic performance data from the platform to produce in the event of an audit to show positive behaviors (like frequent patch) Children's Minnesota is also excited to pursue other business opportunities, using SecurityScorecard as a quick and effective means to access the security posture of any future partner or acquisition.

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