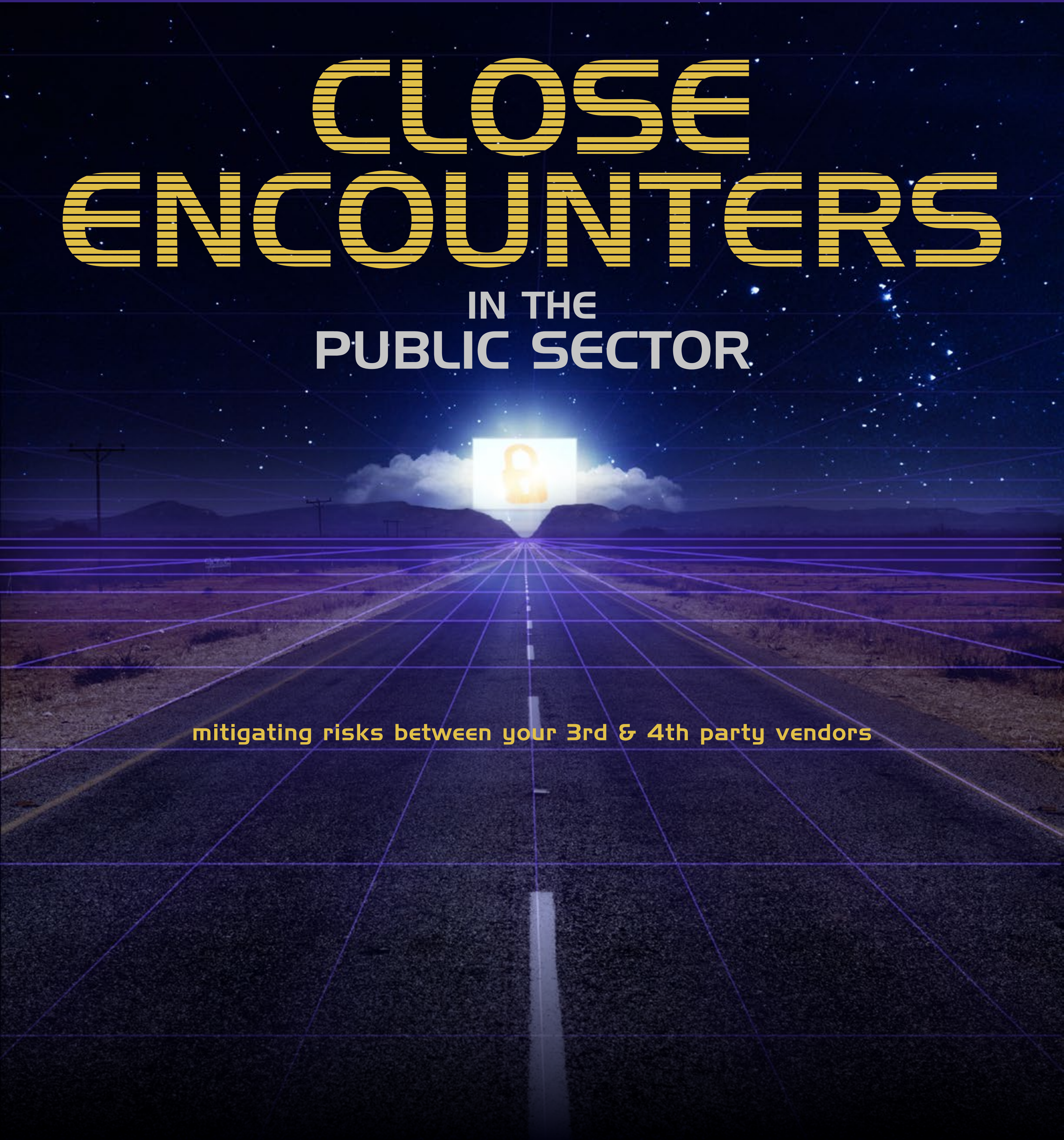
A COLLABORATIVE REPORT BETWEEN SecurityScorecard & Cyentia Institute

CLOSE ENCOUNTERS

IN THE PUBLIC SECTOR



mitigating risks between your 3rd & 4th party vendors

IMPROVING THE CYBER DEFENSES OF YOUR WEAKEST LINKS

SECURITYSCORECARD–GLOBAL LEADER IN CYBERSECURITY RATINGS

THE CYENTIA INSTITUTE–EXPANDING CYBERSECURITY KNOWLEDGE

Introduction

It is often said that cyber defenses are only as strong as the weakest link, which applies equally to individual organizations and to their supply chains. Headlines of breaches stemming from third and fourth parties routinely testify to the truth behind the adage. As a result, most public sector organizations know the risks imposed by these "close encounters". But what can be done about those risks?

SecurityScorecard and the Cyentia Institute recently teamed up to analyze data collected on over 230,000 organizations for clues about the underlying conditions exacerbating third- and fourth-party risk. We measured the extent of digital supply chains, investigated the prevalence of security incidents among third- and fourth-party vendors, and explored the effects of that exposure to gain insights on better managing risk.

This document summarizes key findings from that research using a subset of the data focusing on 7,347 public sector organizations.

Data for this analysis comes from SecurityScorecard's Automatic Vendor Detection capability. Automatic Vendor Detection provides the industry's only cybersecurity risk score for your fourth parties and the entire supply chain.

CONTENTS

From the Headlines:

The massive SolarWinds supply chain hack that came to light in late 2020 sent shockwaves throughout the public sector. SolarWinds Orion is an IT monitoring system with privileged access to many customers' log data, performance data, and other parts of their network. Starting in 2019, malicious threat actors gained unauthorized access to the Solarwinds network, eventually injecting malicious code called "Sunburst."

The Sunburst code was then included in Orion updates pushed to more than 18,000 organizations in early 2020. Numerous local, state, and federal agencies were affected, prompting the U.S. Cybersecurity & Infrastructure Security Agency (CISA) to issue an Emergency Directive. Despite its unprecedented scale, the sophistication of Sunburst helped to provide attackers unfettered access to its victims for over a year.

Relevant to this research, the SolarWinds attack illustrates the dangers of our increasingly-interdependent digital supply chain. Every technology, service, and third party is added for a purpose, but every one of those additions also increases exposure to risk.

Digital Supply Chains in the Public Sector

Let's dive in and look at how the public sector stacks up against other industries when it comes to third-party risk..

Column 1 shows the average[1] number of direct third-party vendors detected per organization. The public sector ranks near the bottom, with an average of 8.5 vendors (although 10% of agencies exceeded the 70 mark[2]). That's about one-third of the digital supply chain relationships typically maintained by information services firms.

WHY DOES THAT MATTER? Each of those relationships represents exposure to various forms of cyber-related risk. Maybe constituent data shared with a vendor is exposed when their systems are breached. Third-party tools might be compromised, giving bad actors a backdoor into your network, similar to what happened with SolarWinds Orion. Or maybe the use of an insecure hosting provider tarnishes your reputation for security due diligence. The list goes on. Of course, having fewer vendor relationships doesn't necessarily mean less risk because many factors are at play. For example, heavier regulation of government agencies generally translates into higher due diligence and compliance requirements when managing digital supply chains. Also, remember that most organizations in the public sectors aren't large federal or central institutions - they're local and state-level agencies with smaller Internet footprints.

> *"Each third-party relationship represents exposure to various forms of cyber-related risk – having fewer vendor relationships doesn't necessarily mean less risk."*

Instead of a per-organization metric, Column 2 looks at the aggregate view of third-party interconnectivity across industries. We can quickly see that the public sector supplies only a fraction (0.1% of the vendor relationships in our data). This makes sense because government agencies tend to consume third-party IT services and software rather than provide them to other organizations.

We will hop over to Column 4, which compares the geographic diversity of third-party relationships. This is done by measuring the average number of countries represented among detected vendors. Doing business with a company in another country doesn't automatically increase or decrease cyber risk. However, it does expose organizations to new laws, security requirements, and other geopolitical issues. The public sector ranks at rock bottom for geo-diversity, with digital supply chains spanning an average of 3.3 unique countries. That seems relatively intuitive, given the heavier regulations and scrutiny of vendors mentioned previously. Also, most government agencies have a local or national focus, which lessens the need for international third-party relationships.

[1] The distribution of vendors detected varies greatly among organizations, so distilling it to an average value isn't ideal. The main report shows a fuller range of values for each sector if you're interested.

[2] If some of these numbers seem small compared with other sources you may have seen enumerating third-party relationships, keep in mind the methodology behind this particular dataset. These are vendors visible from outside-in scanning of an organization's internet-facing infrastructure. We're not conducting an exhaustive inventory of upstream and downstream vendors of all types. The presence of a vendor's code running on your website will be detected, but we have no idea who carries your packages—or cleans the office.

Column 3 shifts the focus from third parties to the explosion in fourth-party relationships. To measure this, we counted the number of third parties for each organization and the total number of organizations each of those third parties was connected to (i.e., fourth parties). We then used those tallies to calculate a third-to-fourth-party growth multiplier for every organization. Given the number of third-party vendors detected, the typical organization has indirect relationships with 60 to 90 times the number of fourth parties. In this instance, we can see that the public sector falls right in the middle of that range, with an average fourth-party growth rate of 76x, placing it among the upper half of all industries.

If you're looking for more insight into common technologies represented in the third- and fourth-party relationships we detected, you can find that (and more) in the full report.

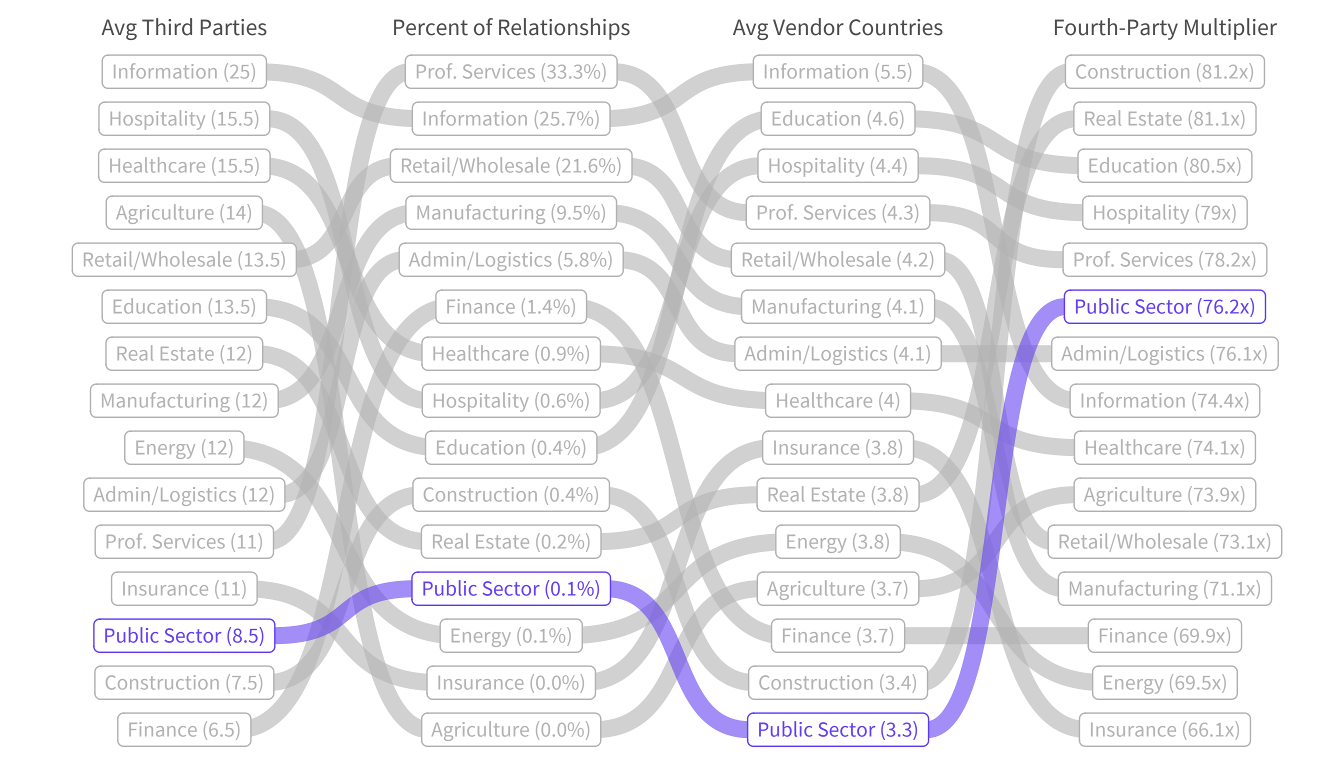


Figure 1: Comparison of key stats on digital supply chain relationships across sectors

Security in the Digital Supply Chain

Given the third- and fourth-party interdependencies we've observed thus far, it stands to reason that those relationships have ramifications on cyber risk for both individual organizations and their broader supply chains. An organization that invests a great deal of effort in securing its own infrastructure could see those efforts undermined by vendors that don't maintain a similar level of security. Thus, we want to bring up a critical question: **ARE PUBLIC SECTOR ORGANIZATIONS MORE OR LESS SECURE THAN THEIR PRIMARY VENDORS?**

Although we can't answer that question specific to your organization in this study[3], we can address it generally across the 235,000 organizations in our sample. We leverage ratings determined by SecurityScorecard as our measure of security posture for all first-party organizations and their third-party vendors. Figure 2 compares the breakdown of scores for each group.

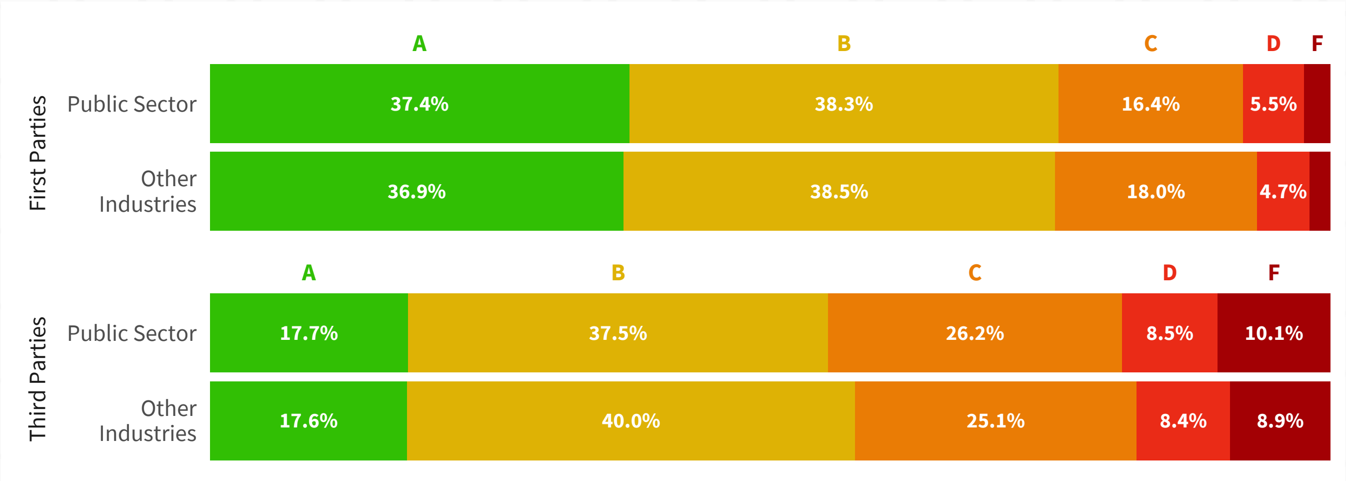


Figure 2: Comparison of security posture ratings for first and third parties

The results justify concerns regarding the security posture of third-party vendors. Public sector organizations achieve the highest security rating of A twice as frequently as their third-party vendors (37.4% vs. 17.7%). On the other end of the rating spectrum, third parties are nearly five times more likely to receive an F on their scorecard than the agencies they supply (2.4% vs. 10.1%). This is not great news, but not entirely unexpected for those familiar with third-party risk management. Plus, the findings for the public sector in Figure 2 mirror what we see in other industries.

At this point, you may be thinking, "Who cares about third-party security grades—breaches are what really matter to my organization!" SecurityScorecard had the same question in mind when their analysts determined that firms with poor security ratings were up to 7.7 times more likely to experience a breach.

[3] But you CAN begin answering this question for your organization with a free SecurityScorecard account.

Breaches in the Digital Supply Chain

The top chart in Figure 3 presents a statistic that hammers home the point about organizational interdependence and exposure to cyber risk: 98.5% of public sector organizations have a relationship with at least one third party that has experienced a breach in the last two years.

The bottom chart contains another equally jarring statistic: Half of all agencies have indirect relationships with at least 176 fourth parties known to have had breaches in the last two years.

This doesn't mean that those organizations were involved or impacted by those breaches. It doesn't even mean that the nature of the relationship between the victim and its third parties is such that the breach could propagate them. But it does mean that nearly every public sector organization is at least indirectly exposed to risk through circumstances outside their control.

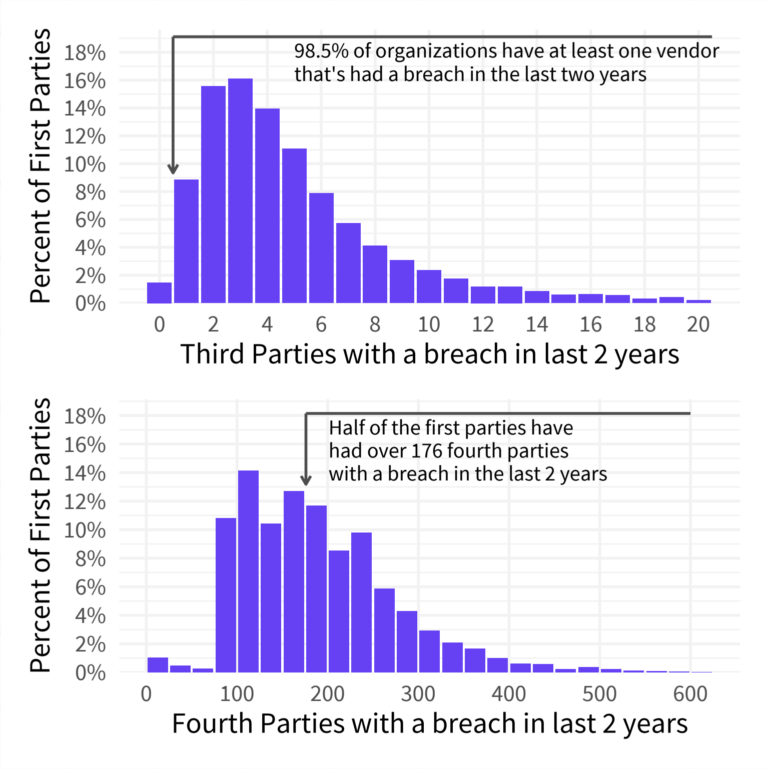


Figure 3 (left): Exposure to breaches via third- (top) and fourth- (bottom) party relationships

SO, WHAT DOES THIS ALL SIGNIFY?

Third- and fourth-party vendors have become necessary for organizations' digital supply chains, but that doesn't mean your organization is one moment away from becoming a headline. What it does mean is that organizations in the finance sector must be aware of the third- and fourth-party relationships they do have and maybe even consider putting rules and processes in place to ensure that those connection points stay secure. Keeping up to date on patches and updates, as well as having a point of contact with your third parties, can be a good way to ensure your organization is doing as much as it can to keep its cyber risk in check.

To learn more about how you can mitigate your cyber risk across 3rd & 4th party relationships, read the full report.

A COLLABORATIVE REPORT BETWEEN
CLOSE ENCOUNTERS
OF THE
THIRD (AND FOURTH) PARTY KIND
IMPROVING THE CYBER DEFENSES OF YOUR WEAKEST LINKS
SECURITYSCORECARD-GLOBAL LEADER IN CYBERSECURITY RATINGS
THE CYENTIA INSTITUTE-EXPANDING CYBERSECURITY KNOWLEDGE