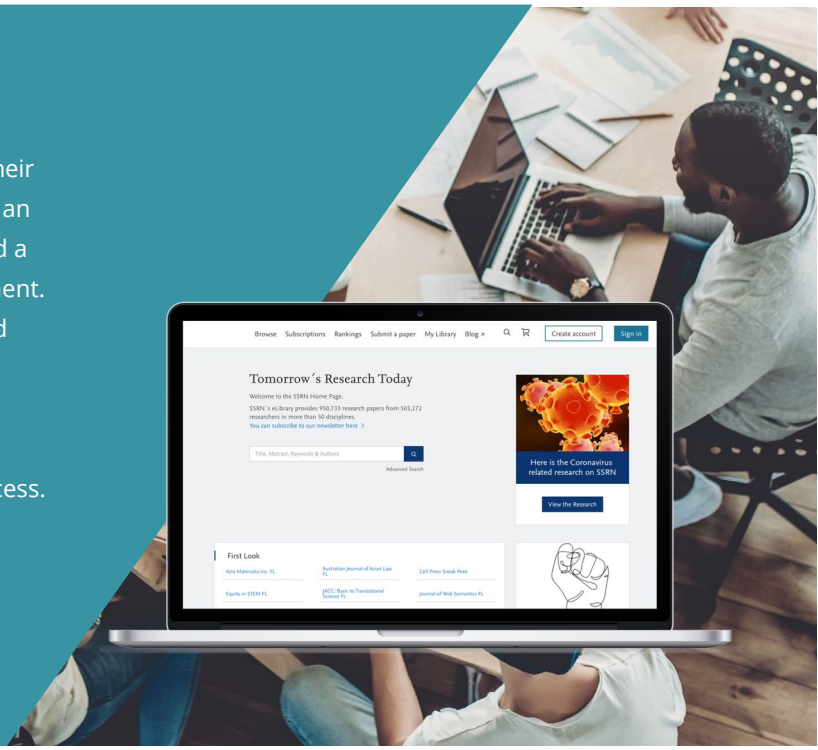
ELSEVIER/SSRN

EXPERTISE AND ATTENTION TO DETAIL DELIVER PCI COMPLIANCE AND PROTECT CLIENT REVENUE

SUCCESS STORY

Elsevier/SSRN reached out to ITX Corp. for help in certifying their compliance with PCI requirements. Committed to delivering an even higher level of quality, our team of testers incorporated a comprehensive assessment of the client's security environment. Through good old-fashioned 'white hat' hacking, we detected numerous potential vulnerabilities, including one high-risk exposure tied directly to client revenue. ITX prioritized each threat to accelerate mitigation, not only improving SSRN's application security but protecting client revenue in the process.

PCI COMPLIANT



MEET THE CLIENT

Elsevier ($2.5B annual revenue) is the parent company of SSRN, formerly known as Social Science Research Network. SSRN is devoted to the rapid worldwide dissemination of research. Through continuous innovation, they focus on creating tools that enhance researcher workflow and productivity, building bridges to close the divide between the previously separate worlds and workflows of working papers and published papers.

FEEDBACK

"Technical compliance projects are challenging....The final testing phase was particularly tough, but ITX did a brilliant job managing all the complexity. I was extremely impressed by how the team handled a critical infrastructure build that involved so many moving parts – and we're delighted to have achieved PCI compliance with ITX's expert help."

— ***Michael Parsons,*** *Director of Product Management, SSRN*

GOAL

Provide compliance with a new PCI requirement by conducting penetration tests of SSRN's application security environment. Capitalize on the opportunity to detect, report, and mitigate potential vulnerabilities. Reduce client risk and boost client confidence by identifying and prioritizing each threat to facilitate remediation or mitigation.

STRATEGY

The ITX Testing team conducted a manual penetration test – relying heavily on the expertise and diligence of ITX testers drawn from QA, Engineering, Development, and Security – instead of automated scanners. No special technology was required — just thorough hacking using well-established tools and techniques to pinpoint potential vulnerabilities and access points. The team then prepared a report summarizing our methodology and collaborated with the client on assessment, prioritization, and mitigation.

UNDERSTAND THE PROBLEM

- Confirm SSRN's compliance with new Payment Card Industry (PCI) requirement.
- Take advantage of the opportunity presented by the "pen test" to identify security vulnerabilities in SSRN's application and system environment.
- Establish and share with SSRN a formalized process for prioritizing unmitigated threats into their backlog.

IMPLEMENT TARGETED SOLUTIONS

- ITX mobilized a team of highly experienced testers, drawn from four internal disciplines, to provide a 360-degree risk assessment of the client's environment.
- Our team of "white hat" hackers conducted a manual penetration test to detect vulnerabilities that automated scanners could not find.
- We then populated the client's backlog with a list of potential and active threats; our risk-based approach helped to prioritize remediation.

RESULTS

- **ITX's team of 'white hat' hackers detected numerous potential threats, including one high-risk vulnerability.** By prioritizing their mitigation, we not only improved SSRN's security environment; we also helped them protect significant client revenue.
- ITX went the extra mile by incorporating a comprehensive threat assessment into a PCI-required compliance test – **boosting client confidence in their system security and in ITX as a strategic partner.**

Secure Network and Systems | **PII Protection** | **Vulnerability Management** | **Access Control** | **Monitoring and Testing Practices** | **PCI Compliance**

1 South Clinton Avenue, Suite 900, Rochester, NY 14604 | 585.899.4888 | 24x7x365: 800.600.7785 | www.ITX.com