



## CUSTOMER CASE STUDY

“NeXpose gives us a wider view of what’s happening, as it assesses all IT systems and devices across the organization, including Web applications, databases, firewalls, switches and routers.”

Adam Pearson  
Information Security Manager  
Lone Star National Bank

## NeXpose Optimizes Risk Assessment for Lone Star National Bank

Financial services institutions are under more pressure than most organizations to ensure their networks, databases and overall computing systems are secure and protected from intrusions that could lead to data tampering or theft. Their security challenges include mounting government and industry regulations, regular audits, identity theft and numerous other threats. Because they store customers’ financial records and other private and sensitive information, compliance with the Gramm-Leach-Bliley Act (GLBA) is critical, as is scanning for vulnerabilities and factoring their risk to the financial institution’s environment.

At Lone Star National Bank, a full service, independent community bank with total assets exceeding \$1.6 billion dollars, the information security team considers risk assessment one of its highest priorities and sought a tool that has the ability to both factor and report on risk. The team found that among all the vulnerability scanners available on the market, only Rapid7’s NeXpose provides risk factoring, as well as comprehensive information to perform focused and effective patch management. With the ability to automatically determine risk factors, Lone Star National Bank saves half the time and money it once spent to manually research its networks and systems and find the vulnerabilities that need to be fixed.

### Situation

Lone Star National Bank has branches across the Rio Grande Valley of Texas, including its corporate headquarters in Pharr and the data center operated by the information technology department in McAllen. When information security manager, Adam Pearson, and his team found themselves increasingly challenged by several time-consuming manual tasks, IT risk assessment was foremost among them. To formulate risk factors, the team had to take code and analyze it manually, often coming up with imprecise results.

Pearson went searching for a product that could provide comprehensive, corporate-wide risk assessment and actionable information for effectively performing patch management. That search took him no further than NeXpose, Rapid7’s vulnerability assessment and risk management solution.

### Solution

Lone Star National Bank purchased both internal and externally-hosted scanning services to ensure thorough scanning of both external customer-facing Web networks and internal IT and restricted financial environments.

“NeXpose gives us a wider view of what’s happening, as it assesses all IT systems and devices across the organization, including Web applications, databases, firewalls, switches and routers,” states Pearson. “We run many different services, business process management software and protocols on the network, and we have a variety of servers and operating systems. All of these can be scanned for vulnerabilities, which was a major reason we chose

NeXpose.”

Another important aspect for Lone Star National Bank is NeXpose’s risk management capabilities.

“NeXpose provides immediate scan reports containing risk factors, even risk factors of devices, which other vulnerability scanners do not do,” states Pearson. “We can obtain a complete risk management profile on a system in a matter of minutes. The information is broken down by department and group, and it addresses areas that need to comply with financial and banking industry regulations, particularly GLBA (Gramm-Leach-Bliley Act). We obtain all the data we need to prepare for a regulatory audit.”

NeXpose also provides “proof of vulnerability,” verifying that the vulnerabilities found are not false positives.

“False positives can eat up time spent researching them,” states Pearson. “With NeXpose, we can be certain that the scanning results are accurate and none of the vulnerabilities uncovered are false positives.”

NeXpose also allows Lone Star National Bank to generate a detailed remediation plan, including timeframes for achieving resolution. The plan is sorted by system and outlines the steps for remediating each device. The plan prioritizes the areas targeted for remediation based on the assigned risk factors.

NeXpose’s software report presents Lone Star National Bank with information on how many workstations are running different operating systems and what the service levels are. NeXpose also informs IT when software needs to be updated and system versions are out of synch, helping to keep the entire IT environment current.

“There isn’t a reporting tool in NeXpose we don’t use,” explains Pearson. “The product makes it possible to extract a wealth of information, and we can take that data and drop it into spreadsheets with graphing.”

Although NeXpose offers a broad range of scanning and reporting capabilities, Lone Star National Bank has found NeXpose very easy to use, and it was also simple to set up.

“You can set it up according to how your organization is structured and operate it from a centralized location,” states Pearson.

## Benefits

Lone Star National Bank’s experience with NeXpose has gone beyond its expectations. In addition to providing an extensive array of risk management tools, broad flexibility and increased awareness of the status of the bank’s IT environment, NeXpose has delivered tangible benefits leading to a tremendous return on investment:

- **Time Savings** - Lone Star National Bank now scans its organization and obtains risk factors in half the time that would be consumed with another system. The information security team saves time researching vulnerabilities, determining what needs to be fixed and generating reports.
- **Cost Savings** - Lone Star National Bank saves money as a result of saving time, as the resources devoted with its previous risk management system can now be focused elsewhere.
- **Streamlined Operations** - The IS team’s time management is optimized now that the frustration of manual and time-consuming risk assessment is removed. With the comprehensive NeXpose remediation plan, patch management is conducted and completed much faster and more thoroughly. The executive reporting helps management to determine what needs to be addressed and to prioritize appropriately.



In addition to expressing his appreciation of NeXpose's solid functionality, Pearson proclaims, "NeXpose is a fun tool! We find it easy to understand; therefore we can use it to its full potential. We can implement it so the entire IT staff benefits. The Help Desk can now identify issues and know what's happening whenever an event occurs."

### **About Rapid 7**

Rapid7 is a leader in vulnerability management and compliance, delivering a single unified solution across an organization's entire infrastructure. Rapid7 NeXpose helps securities professionals to reduce their attack surface by providing actionable insights into the real threats from vulnerabilities across their entire IT infrastructure. Rapid7 NeXpose is the only solution that provides in-depth coverage of vital Web and database systems in addition to networked devices, servers, and operating systems. The NeXpose A.I. and Reporting Engines synthesize large quantities of raw data to provide direct insight into the vulnerabilities that represent the most risk to the business. From this insight the product delivers a set of prioritized remediation recommendations that help security professionals get protection fast. Organizations, including Black & Decker, Trader Joe's, Florida State University, the New York Times, and the City of Philadelphia, continually rely on Rapid7 products and services to mitigate risk and remain compliant. For more information, go to [www.Rapid7.com](http://www.Rapid7.com).