



CLIENT SUCCESS STORY



Guaranteeing the security of client information is a requirement of doing business for St. Louis company

Handling billions of dollars of client funds and more than 20 million transactions a year has Cass Information Systems placing an extra-high value on security—so much so that the nation's leading freight invoice and management information processor is investing in regular third-party security assessments conducted by Advanced System Designs (ASD).

Established in 1906, Cass has three major business segments (transportation information systems, utility information systems, and Cass Commercial Bank) with offices in St. Louis, Columbus, and Boston. Clients include Fortune 500 companies like Ford, Nestle, Dow Chemical, Mercedes, and others.

"In its simplest form, we collect freight and utility bills from clients and handle payment for them," says Jeff Thurston, Vice President of Information Technology at Cass. "Our clients are outsourcing a process and want to be assured we're keeping their financial data secure. The same is true of our commercial bank clients. Our goal is to meet or exceed these expectations."

Preventing problems before they happen

Because Cass operates a commercial bank, its systems are annually audited by the Federal Reserve Board. The company also has an internal auditing group that conducts regular assessments. Security has never been a problem, but since technology changes so frequently, each day brings new challenges. With new reports of viruses, worms, and security breaches, Thurston wanted to fortify his existing defenses. He decided it was time to supplement internal audits with an independent, third-party assessment.





“It seems irresponsible not to have an independent perspective on what we are doing. New security threats emerge every day. We can’t have the attitude that it won’t happen to us. We must remain vigilant.”

Cass Information Systems
Senior Networking Engineer—**Sean Mullins**
Vice President of IT—**Jeff Thurston**

“I see these security assessments as an insurance policy. We don’t have problems now and I don’t anticipate we will, but it seems irresponsible not to have an independent perspective on what we are doing,” Thurston says. “New security threats emerge every day. We can’t have the attitude that it won’t happen to us. We must remain vigilant to ensure our security practices are adapting to these threats. ASD can help because they have a unbiased perspective.”

“Hacking” for a good purpose

The vulnerability assessment begins with an analysis of more than 75 servers, network devices, and applications to quantify risks that may lead to the compromise of Cass’s systems. One technique called white-hat hacking has security experts pretend to hack into Cass’s systems from the outside. It’s an effective way to find exposures—and a process most companies don’t have the tools or expertise to perform themselves. ASD also evaluates Cass’s security practices against top exposures defined by groups such as SANS, the FBI, Gartner Group, and others.

Once data collection and analysis is complete, ASD prepares a report that identifies each exposure, then explains why it is a problem and what can happen if it isn’t addressed. Also provided are best practices related to each identified issue, offering suggestions Cass may want to consider as remedies are explored. Each finding is assigned a severity rating to help Cass prioritize remedial efforts—five stars, for example, indicates an exposure that warrants immediate attention.

According to Alan White, Security Team Leader at ASD, “The first step in protection for online resources is locating where information is stored, understanding the security measures in place that guard that information, and identifying vulnerabilities and suspect configurations that place information at risk. Our vulnerability assessment solutions work to provide critical knowledge and advanced warning of potential online security risks across network, server, database, and wireless operations.”

Thurston agrees. “ASD’s process is more comprehensive and tailored to our needs. They highlight areas we can concentrate on and improve, instead of recommending a blanket approach that may result in wasted efforts.”

Protecting the IT investment

One key part of ASD’s security process is an availability assessment, in which security experts review solutions and disaster recovery plans in place to keep systems up and running and to back up and recover data. Cass, for example, has “redundant” systems—if one server goes down, there’s another one ready to take its place.

“We’ve invested millions of dollars in the equipment required to keep our systems highly available. We want to make sure that availability is not compromised,” Thurston says. “The availability portion of the assessment is important because our clients access our information delivery services in the performance of their jobs. If there’s a problem, it doesn’t just affect us—it affects our clients as well.”

Balancing security and business

Cass defines its core competencies as data acquisition, data management, information delivery, and financial exchange. Security is an integral part of these competencies. That’s where ASD comes into play.

“We value security and spend considerable resources to protect client information,” Thurston says. “Everything we do has an element of security that needs to be considered to ensure that information flows to and from our clients in a secure and reliable way. ASD helps us by providing highly specialized personnel and tools that extend our internal capabilities.”

In fact, ASD is one of just a few companies with security expertise in the many platforms Cass operates—iSeries, HP Tandem, Unix, Linux, and Windows. “The whole point of an assessment is to look for exposures throughout the company,” Thurston says. “If you hire a firm that can only assess one or two platforms, then you’ve left a gap.”



- Technology**
- People**
- VPN/Firewall
- Authentication
- Spam Control
- Internet Management
- Intrusion Detection
- Audits & Assessments
- Traffic Management
- Security Appliances
- OS Security
- Anti-virus
- Business**
- Results**

Technology People. Business Results.

ASD people are technology people. Experts who understand the breadth of technology solutions available. Consultants who apply that expertise to your specific needs. And partners who care about delivering business results for your organization. For more information or to arrange a meeting, give us a call or visit us at www.asd.net/security.

Our security offerings range from assessment, design, and implementation services to product sales and support. A leading provider of security expertise and solutions, we help you protect information, secure applications, securely connect remote workers and business partners, control Internet usage, and detect and block malicious code.

St. Louis office
866.ASD.9406
or 314.317.9406

Corporate office
877.ASD.4968
or 309.263.7944

To ensure Cass has no gaps, and to keep security at today’s ultra-high level over time, Thurston plans to have ASD conduct regular security reviews.

“Security is a balance that everyone must find for their own business. For us, it’s having enough security to protect ourselves and our clients without imposing excessive inefficiencies to our operation. ASD is helping us maintain that balance.”