

InfoExpress Case Study

Company



Ulster Savings Bank
www.ulstersavings.com
(800) 762-0449

Business Mandate

- Increase network stability while mitigating regulatory compliance audit and security risks
- Find a solution that would help secure Ulster's network from internal threats
- Ensure that every machine on Ulster's network is compliant with corporate security policies and guidelines

Return on Investment

- Total Cost of Ownership for 315 seats = \$40,000
- Risk Mitigation ROI = \$500,000 (Regulatory Penalty Exposure) + \$5 million (Customer Information Security Exposure)
- Network and Workstation stability value = At least 5% improvement. Approximately \$50,000 annual return in recovered personnel productivity
- Experienced 15-20% fewer help desk calls

Ulster Savings Bank Adopts InfoExpress CyberGatekeeper to Secure Corporate Network

Overview:

Established in 1851, Ulster Savings Bank has over 20 locations throughout New York State. The bank also owns and operates USB Agency Tax & Financial Services and Ryan Insurance. In total, Ulster Savings Bank employs over 350 people and manages over \$625 million in assets.

Security Challenge:

For companies that must comply with government or industry regulations (Gramm-Leach-Bliley, Sarbanes-Oxley, HIPAA, PCI-DSS), a thorough IT governance framework, with iron-clad security is a necessity to ensuring audit and regulatory compliance. This is especially true for financial institutions. Aligning, implementing and enforcing security guidelines, policies, processes and procedures throughout a rapidly expanding organization can be a daunting task. Ulster Savings Bank recently faced this challenge head on.

Every year, Ulster Savings Bank hires a third party company to perform an IT security audit and discover flaws, shortcomings and vulnerabilities in its network. In 2005, the third party conducted port scans, hung sniffers on the network while simulating malicious activity and monitoring how well the network responds. Software security patches on all network nodes were also probed using this method.

Ulster Savings learned that their security measures were rock solid when defending attacks from outside their network. However, the bank discovered that the same tests conducted from inside the corporate firewall were not as encouraging. The development and enforcement of an enhanced security architecture encompassing internal network access would be a necessary step to ensure the bank's network integrity. Having endpoint visibility and the ability to enforce a standard compliant configuration of endpoint devices were viewed as necessary elements of the enhanced security framework.

Furthermore, Ulster recognized the need to continually evolve their governance policies, processes, and network infrastructure in order to proactively maintain network integrity and mitigate risks from data theft, leakage and loss. Avoiding compliance violation penalties, legal exposure and more importantly, safeguarding sensitive proprietary and customer information were (and are) essential.

Ulster Savings thereby realized that they needed a comprehensive solution that included internal intrusion detection and policy enforcement, including end-point configuration management.

InfoExpress Solution:

Jim Hochstatter, vice president of technology for Ulster Savings,

Solution

- Ulster Savings Bank is utilizing InfoExpress' CyberGatekeeper to:
 - Grant network access only to compliant endpoints
 - Quarantine rogue endpoints
 - Monitor real time network activity
 - Implement software patches version control and monitor patch levels throughout the network
 - Ensure that every machine connecting to their network is approved

Customer Comments

- "The trust of our customers is of the utmost importance to us. With CyberGatekeeper, we know that our customers can trust that our network and their personal information is safe from threats."
 - Jim Hochstatter, VP of Technology for Ulster Savings Bank

determined early on that the ability to standardize security guidelines, policies, processes and procedures for current users, new builds and new employees was of paramount importance. In addition, the solution he was looking for had to be able to standardize and update software patch levels throughout the organization, all while quarantining machines that were not compliant. It was essential for Hochstatter that he be able to monitor each computer connecting to Ulster Savings' network to ensure it was up-to-date and compliant with sanctioned standard configurations.

After evaluating several solutions, Jim Hochstatter chose the InfoExpress CyberGatekeeper solution. CyberGatekeeper protects his bank's network from rogue users and therefore helps avoid financial penalties associated with failing audits. Jim felt confident that CyberGatekeeper could bolster the reliability of his network and ability to enforce internal controls for Sarbanes-Oxley compliance given the thorough audit trails provided by the InfoExpress' solution. CyberGatekeeper ensures that all endpoints on the network are visible and monitored. CyberGatekeeper technology improves the accuracy of the organization's audit trail, provides custom reports, and automates portions of the data collection process

After deploying InfoExpress' CyberGatekeeper to protect their corporate network and \$625 million in assets, Ulster Savings took a conservative approach to installing the solution. In just under five month's time, CyberGatekeeper was fully operational and protecting every Ulster Savings desktop and laptop computer. Installation took place much faster and easier than expected, and was completely transparent to each user.

"With InfoExpress' CyberGatekeeper integrated into our network, we have created a superior level of network security and visibility," said Hochstatter. "CyberGatekeeper used in conjunction with 802.1x gives us the ability to verify that every machine talking to our network is compliant and allows us to avoid dangerous rogue machines that can get in and damage corporate assets."

CyberGatekeeper allows Hochstatter and his team to take snapshots of network activity to analyze traffic and better understand what is running across Ulster's network. "Proper implementation of the CyberGatekeeper NAC solution does more to evolve your network to run less like a KIA and more like a Mercedes-Benz than any other single tool can."

Even though the bank does not have a large number of mobile users, the new system enforces configuration standards prior to system access when laptops are connected to the internal network.

Return on Investment

At Ulster Savings, the CyberGatekeeper deployment, as well as integrator fees and internal staff time at Ulster Savings Bank, totaled less than \$40,000 for 315 seats. Since the deployment helped to ensure each endpoint was compliant with corporate security policy, helpdesk calls have been reduced dramatically. Hochstatter says that calls have been reduced by about 15-20 percent, which reduces helpdesk costs by

about \$40,000 annually.

The biggest return for Hochstatter has been the ability to avoid regulatory fines. Regulatory exposure fines begin at a cost of \$500,000. In addition to that initial fine, customer information exposure usually incurs a cost of nearly \$5 million as well. These figures do not account for civil suit litigation and settlement costs, or for loss of customers or tarnished brand reputation.

Conclusion:

Ulster Savings Bank is now assured that their security policy is strictly enforced throughout their network. CyberGatekeeper gives Ulster the ability to know that its customers' personal information is safe from both internal and external threats. The ability to easily and efficiently scale configuration management and security policy enforcement to new employees in new locations will prove especially helpful as Ulster Savings Bank continues to grow.

Most importantly, Ulster Savings has achieved their need for network endpoint visibility. This ability has helped to ensure that Ulster is in compliance with regulatory and audit requirements.

"Deployment of the InfoExpress CyberGatekeeper Server and Agent was seamless and integrated easily utilizing 802.1x authentication and Microsoft IAS into Ulster Savings Bank's current network, server and desktop environment," said Jeff Jones, managing partner for Topgallant Partners, a New England based technology services company that is InfoExpress' channel partner for the Ulster solution. "CyberGatekeeper provides real-time policy enforcement, but most importantly provides Ulster Savings clear visibility into the end-user's desktop which in most organizations today is fuzzy at best."