CASE STUDY
CITY OF STOW

IMPROVING NETWORK SECURITY

HOW AN INFORMATION ASSURANCE PROFESSIONAL ASSESSMENT HELPED THE CITY OF STOW

The City of Stow, Ohio is a community of just under 35,000 people, located 35 miles south of Cleveland and part of the greater Akron metropolitan area. In many ways, Stow is an archetypical American community. Those in its local government are in the same position as the staffs in hundreds of other smaller cities and towns across the country – doing their best to stretch limited cash and finite human resources to cover all the services their constituents need and expect.

CUSTOMER PROFILE
City
- 35,000 people
- Located 35 miles south of Cleveland

THE SITUATION

Dale Germano, Stow's Manager of Information Systems, is one of those trying to do more with less. He and his staff are responsible for all the City's computer systems and networks, including those in City Hall, the Safety Building, remote Fire Stations 1 and 2, and the Parks Department. Germano was appointed Stow's Information System's (IS) Manager in 2009, but because he came up through the ranks, he is well aware that the IS function has been stretched thin for a long while. Keeping Stow's various systems operating has always been the first order of business. Keeping them secure might be the next most critical priority, but most days, a second-place priority gets little more attention than last place.

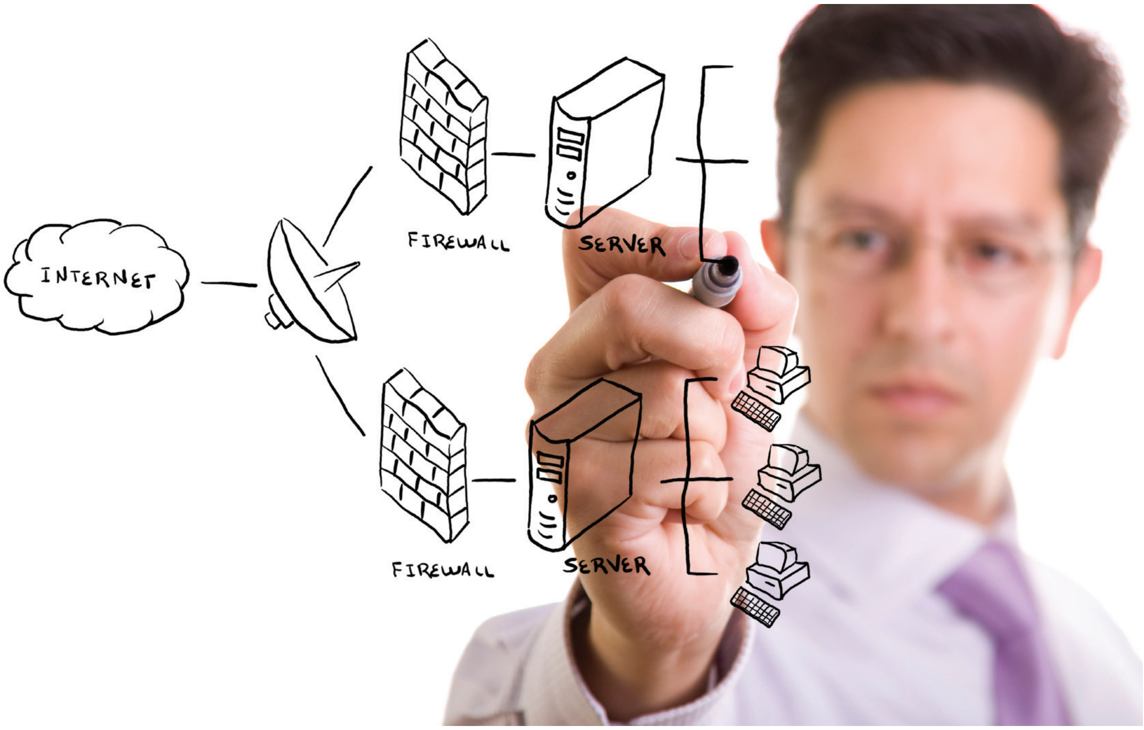
THE CHALLENGE

Like other local governments in communities of every size, the City of Stow relies on advanced information systems to help deliver key services to its residents. With that reliance comes a clear responsibility to protect information confidentiality, integrity and availability. The City's Human Resources and the Fire Department maintain information that is required to be protected by the Health Insurance Portability and Accountability Act (HIPAA). The Police Department is connected to Ohio's Law Enforcement Automated Data System (LEADS), which requires stringent security controls. The Finance Department retains tax records full of sensitive and confidential personally identifiable information that must be kept private.

"Frankly," says Germano, "I was worried that if any of these regulatory and reporting agencies asked for a security audit, we simply couldn't pass. That could mean big fines that no city our size could manage easily. Even worse, what if we had an actual security breach? How many of our friends' and families' lives might be affected? What kinds of legal liability would we have? What could we be facing in terms of loss of reputation, loss of community confidence, loss of status?"

To bring Stow's IS security compliance up to standards, Germano fully expected to need additional funding. So he wanted answers that he could attach to real numbers. "Motorola's security experts told me they could identify and assess security weaknesses across all our systems, comprehensively. They would tell us which were the most urgent problems, how to fix them, what it would cost to fix them, and how much it could cost us if there were an incident before we fixed them. That is precisely what I needed to build a business case for investing more in IS security."

So the City of Stow engaged Motorola Security Services to prepare an Information Assurance (IA) Professional Assessment of its IS security posture.



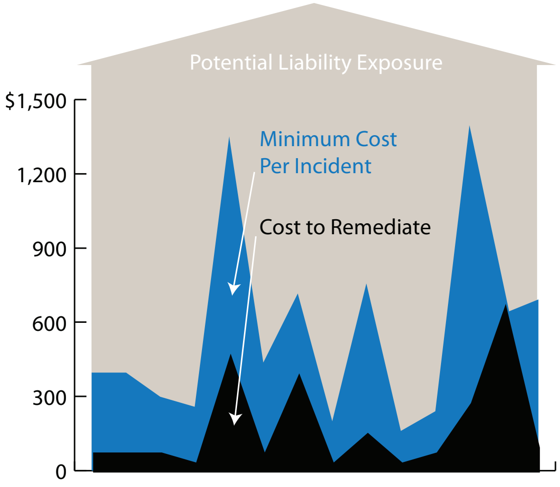
THE SOLUTION

Motorola's IA Professional Assessment Services team recognizes that no technical solution can make a network any more secure than the processes and mindsets of the people who use it. Our IA Professional Assessment takes a holistic look, not only at hardware and software, but at how people work. Our goal is not merely to help better secure your system today, but to help your organization develop a better overall security posture – so you can continue to keep your information assets safe in the future.

The IA Assessment:

- Identifies key assets at risk and potential impacts to core network and functions
- Analyzes risk and threat, mapping findings to key business and operational assets
- Provides actionable, prioritized recommendations for gap closure with recommendations that are prioritized based on the risk to overall operation
- Offers an in-depth final report to ensure that you fully understand the findings, their impact to security, and the recommendations for gap closure

Motorola Security Services experts went to Stow, Ohio. They spoke with key personnel, visited sites that housed critical infrastructure elements, and then explored, locally or remotely, the primary servers, operating systems, applications and access points that make up the City's information system. They even looked into devices in all the sub-networks beyond the primary data center.



After the team had gathered all key data, they went off-site to analyze the City's vulnerability. Motorola identified critical databases that required protection, considered who and how that information could be accessed, identified weaknesses in the City's technical protocols, daily procedures and systemwide policies, then prioritized the threats.

Germano was presented with a report outlining specific technical security findings, as well as a number of observations about Stow's physical and procedural security policies. Each finding noted which data assets were at risk and why. Motorola also provided estimated costs for remediation and compared them to the estimated cost to recover from a related security incident. In almost every case, the cost to correct the problem was significantly lower than the cost to deal with a single security breach. Finally, the report noted that intangible costs, such as those associated with responding to negative publicity, could run much higher if Stow faced an actual breach.

The City of Stow learned that they do indeed have some very high-risk vulnerability that they wouldn't have known existed. Says Germano, "That may be the most valuable thing about Motorola's assessment service. It's not just focused on locking everything up as tightly as you can – it's focused on improving your overall security posture, knowing what needs to be protected and how to keep it protected. We found out where the real threats are, exactly what data is potentially exposed, and what we need to do to fix it. But we also found out how to maintain a more security-aware organization."

Germano was pleased to hear that addressing the City's security issues would require neither five-figure capital outlays nor significant new technology purchases. In fact, some of the most serious risks to their information systems could be mitigated by establishing and enforcing clear, citywide security policies. With a relatively small investment of time and attention to the areas highlighted in their assessment, the City of Stow can ensure that their information is safe, their networks are secure and their risks are minimized.

THE RESULTS

Germano and his team are already planning to go forward with the recommendations offered in their assessment. “Finding the equivalent of a week or two of extra man-hours may not be easy,” says Germano. “But our security assessment lays out a pretty clear plan that shows exactly why it’s important.”

He also notes, “I know we aren’t the only ones who have this kind of problem. There are so many small cities and towns out there, with hard-working folks just like us, struggling with limited funds and short staffs, trying to stay ahead of the fires every day. This is such a valuable tool for moving from reactive to proactive mode. We now know precisely where to spend our time for maximum return-on-effort.”

For more information on how Motorola's Information Assurance Professional Assessment Service can help with your network security please visit us on the web at www.motorolasolutions.com/services/government

MOTOROLA