PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

MICHAEL MCGOVERN
SVP, CISO, & CTO, METRO CREDIT UNION

HEADQUARTERS: Chelsea, MA

EMPLOYEES: 300

ASSET SIZE: $1.5 Billion

INFORMATION SECURITY AND DISASTER RECOVERY GO HAND-IN-HAND

Michael McGovern, CISO and CTO of Metro Credit Union, stands in a unique position. He leads the company's security effort, but also holds responsibility for the organization's disaster recovery planning. Within this role he provides regular reports to the organization's Enterprise Wide Oversight Committee (EWOC). The EWOC is comprised of the CEO, CFO, COO and SVP of Operations, each with a strong interest in supporting and advocating for the company's security and disaster recovery programs.

"We meet with the EWOC once a month to go over Metro's information security posture. They want to know about new security threats that are seen by other organizations and out in the wild, areas where we can improve security. This meeting is our opportunity to share important information with the leadership team," said McGovern.

Conversations with the EWOC often become specific as they review data breach prevention tactics and McGovern provides an update on threats and how personally identifiable information is protected. "Discussions with the CEO can get fairly technical. We talk about stats, data and metrics – including, for example, geo-blocking stats," said McGovern. He continued, "We want to make sure the key people in the organization understand information security threats and our objectives."

McGovern's disaster recovery work is strongly supported by the CEO and Board of Directors. "Because we receive the budget we ask for, we have built a strong technology-based infrastructure that allows us to replicate our data offsite to disaster recovery locations in a manner that is close to real-time. When I talk to other financial institutions, as well as auditors, they are surprised at the detail around our disaster recovery plan and the amount of testing we do on a quarterly and annual basis." For McGovern's program, disaster recover covers technology (infrastructure), operations, as well as people. In the event of a disaster, he ensures a clearly defined process is in place that takes into account a number of different scenarios. He commented, "With my CEO and Board of Directors, we talk about recovery point and recovery time objectives. If we had a disaster today, what data would we lose? How quickly could we recover?"

TOUGH LEARNING EXPERIENCES

McGovern's interest in the intersection of disaster recovery and information security stems from his early career experiences. "I have been working in the financial services industry for about 15 years, and before that I was in the technology industry. Years ago, when I was in the high tech field, information security was not much of a concern. We were all concerned about 24x7 employee access and availability. But, I clearly remember my first experience with a virus – It was the Nimda virus and it took our company out for a week or more. It took our company down to its knees and we had to call in a lot of help to clean our network up and get virus-free. That was the first time I realized the huge role information security can play in business and uptime." McGovern also realized the key importance of establishing a thorough disaster recovery plan in preparation for this type of incident.

After learning this valuable lesson while working in high tech, McGovern then moved into his first role at a financial services organization as VP of IT at a large regional community bank. In the position for ten years, McGovern had the opportunity to greatly expand his security expertise. He said, "The financial services industry was ahead of high tech in terms of taking information security seriously and protecting member data. We were subjected to several audits by the state and the FDIC, as well as internal audits. In the early days, compliance was really driving our security efforts and purchases."

VALUE OF CORPORATE CULTURE

Since arriving at Metro Credit Union, McGovern and information security programs in general have evolved to be less compliance-driven and more focused on aligning with the business to ensure positive member experiences and better protection.

"Our role now is to make sure the credit union can perform day-to-day activities in a secure environment," said McGovern. "Our Board is really supportive of making sure we have a strong security posture. They want to know we are doing our best for our members' protection. We have put additional security mechanisms in place and now we are focused on strengthening as much as possible and still allowing our employees to service our members."

McGovern believes in the value of corporate culture and mindset when building out a strong security program, something which starts at the top. His Board represents a skilled and experienced group committed to making Metro Credit Union number one. Furthermore, McGovern reports into a very involved and engaged CEO, who makes security a key priority. He said, "The CEO is involved in all aspects of the IT organization. We connect three or four times a day."

BALANCE IS KEY

One of McGovern's proudest achievements at Metro Credit Union was creating the credit union's disaster recovery infrastructure. In creating this, he pulled on lessons learned and experiences from earlier in his career, while realizing he needed to embrace innovations, such as Cloud technologies. "We built a great disaster recovery solution for my previous employer, but at Metro Credit Union I had to step back and evaluate if that same solution was still valid for Metro's environment. I looked at Cloud technology, which has matured recently. It took me six months to review new solutions and evaluate from a cost and control perspective and put the right solutions in place for a successful disaster recovery program."

Even with broad experience as a well versed leader, McGovern continually works hard to balance traditional IT functions, information security and business continuity planning with a relatively small staff. Because his team is responsible for a diverse set of requirements, he looks to hire well-rounded problem solvers with good time-management skills. McGovern ensures they receive the technical and business training they need to support the solutions in their environment. "We train at least two people on the team in every technology, so we can all collaborate to get our various tasks completed," said McGovern.

PEER COLLABORATION

McGovern commits himself to his own educational growth and continues to keep pace with evolving threats and emerging approaches to information security. He leverages communities like FS-ISAC, Infragrard and ISSA to keep abreast of best practices and to share critical information with peers. McGovern attends monthly sessions at the Federal Reserve Bank to keep up-to-date on cyber threats. He said, "The Department of Homeland Security gave a recent presentation and individuals from the Federal Reserve have given presentations on the threat landscape. These are incredibly helpful forums."

McGovern said the events and exercises that involve peer collaboration represent learning experiences to the success of security programs. Just as critical to McGovern are key vendors and trusted partners that help keep him up-to-date on security best practices and emerging technologies. "It is impossible to manage all the vendors and keep pace with the innovations without help," said McGovern.