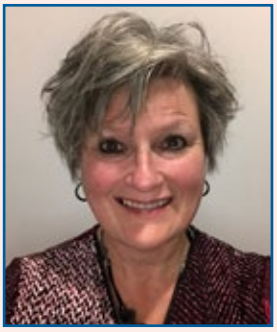
The RIMS Strategic and Enterprise Risk Center presents:

Tina Gardiner
Manager of Risk Management Services
The Regional Municipality of York, Ontario

PUBLIC ENTITY ERM

By Russ Banham



RIMS
The vastness of Tina Gardiner's responsibilities make her work on behalf of the Regional Municipality of York in Ontario, Canada, both challenging and rewarding. Like other individuals entrusted with overseeing ERM for a public entity, Gardiner must communicate and collaborate with a wide range of government employees delivering a myriad of services and programs to 1.2 million residents across York. The Regional Municipality of York consists of nine municipalities located north of the City of Toronto. The local government is organized in a two-tier structure. For example public transit, water, emergency medical services and policing are handled by York Region, while curbside garbage collection, local parks and libraries are the responsibility of each municipality.

Gardiner has overseen risk management at the regional municipality for the past 18 years. York introduced ERM initially as a bottom-up approach and more recently added a top-down process. The framework clearly demonstrated its value, as York received honorable mention for the Global ERM Award of Distinction at the RIMS ERM Conference 2019.

RIMS spoke recently with Gardiner, a member of the RIMS Board of Directors, to discuss how risk and opportunity are integrated strategically across the municipality.

RIMS: What are the special challenges confronting public entities in making ERM effective?

Gardiner: The short answer is the sheer size and scope of York. Large municipalities like ours have so many programs and services they must provide, involving roads and transportation, courts, environmental services, housing, police and, transit, and so on. We also have different tiers of municipal government to contend with. The Regional Municipality of York, for instance, consists of nine local municipalities like Markham, Richmond Hill, and Vaughan, each with its own risk manager. These individuals also have different ERM responsibilities than I have here at the Regional Municipality. I oversee ERM for police and transit, for example, but they handle ERM for fire and recreational services in their respective municipality. Sometimes an automobile accident will occur on a road thought to be my organization's ERM responsibility, but it turns out to have been on a local municipality's road.

RIMS: Do you share each other's best practices?

Gardiner: To ensure consistency in ERM approach, we all meet quarterly through a regional risk managers group, although we're frequently in touch. My organization also belongs to another risk management group involving urban municipalities, composed of risk managers from the City of Toronto and other regional municipalities like Durham and Halton. All of us are spread throughout the Greater Toronto Area, the most populous metropolitan area in Canada. And I also share best practices, documents, techniques and war stories on an online forum with risk managers from small communities and large municipalities across the nation.

RIMS: Aside from the enhanced data sharing, communications and collaborations with local, municipal and peer risk managers, what other recent ERM developments occurred under your watch?

Gardiner: I would point to some of the top-down ERM components we put in place in recent years. For example, we formed a management-level risk committee that led to the implementation of forward-thinking risk management practices, creating statements on risk appetite and risk tolerance. We also created an ERM Playbook documenting the evolution of the ERM program. It has become an indispensable educational resource for staff members and departments, ingraining a culture of risk awareness across all levels and business areas. More recently, we endorsed a variety of ERM efforts to address concerning risks like climate change, cybersecurity and fiscal strategy.

RIMS: Could you elaborate on the Region's cyberrisks—why this is particularly concerning and how ERM is innovatively helping to provide a solution?

Gardiner: Like other government entities, we've been exposed to an increase in cyber threats emanating from hackers and other bad actors. We're also exposed to cyberrisks posed by negligent employees and third-party vendors with access to our systems. My organization must ensure assets like intellectual property, personal data, and physical infrastructures are protected from a data breach. To do that, we needed to collaborate closely with our IT department and colleagues in legal, finance and compliance, given evolving privacy regulations. We formed a team among us to set out what we needed to accomplish, process-wise, to reduce the regional municipality's cyber exposures.

RIMS: What were some of the items on the team's drawing board?

Gardiner: They ran the gamut from procurement contract terms and conditions to employee education and awareness, effective data breach response planning, and the use of IT security tools and [network intrusion] monitoring capabilities.

RIMS: Let's dive in to one of those items. Take your pick.

Gardiner: We did quite a bit of work on the contractual terms and conditions involving our procurement process with cloud-based technology vendors. The team created a cybersecurity questionnaire that vendors must fill out to bid for work. The finished questionnaire is subsequently reviewed by the IT security organization, which passes or fails the vendor. This is embedded in two new tools we developed to assess third-party vendor cyberrisk exposures, which were later endorsed by the region's senior management team for corporate-wide use. The first tool, called CRIT (Cyber Risk Information Tool), is designed to capture information on the vendor's cyber exposures. The team then uses the second tool, CRET (Cyber Risk Evaluation Tool) to review and assess the vendor's exposure information and 'score' it on a traditional heat map. Based on the results, the team may reach out to the vendor for more information or set up a conference call to discuss our concerns. Once we 'greenlight' a vendor, each team member signs off on the decision as a risk owner.

RIMS: You had mentioned data breach response planning. Can you describe some of the work done by the cross-functional team to respond to evidence of a data breach?

Gardiner: The team worked closely with the regional municipality's insurance broker and our internal data breach coaches and forensic specialists—in putting forward the data breach plan. It mirrors our emergency response plan, with the same definitions and levels of engagement. The reason is that a data breach is another type of 'emergency.'

RIMS: Has the plan proved effective? Has a data breach occurred that was headed off at the pass, so to speak?

Gardiner: Funny you ask that. We actually experienced a data breach within the organization a couple years back. We were part of a pilot program evaluating the value of people working from home on a remote and virtual basis. The cyberrisk team was already in place and had developed the CRIT and CRET tools, though we were still in the early days. Anyway, one of the remote workers looked up a staff member's name using a search engine. She wanted to find the person's extension to electronically send an insurance claim. While looking up the name a series of invoices from an insurance adjuster popped up on her screen. She could see private details involving claimants and their doctors and lawyers, a serious privacy issue. She contacted me and I went in and got the same results.

RIMS: What happened next? Was the data breach plan put in motion?

Gardiner: In a word, yes. The IT security member of the team was notified immediately and he shut down our entire claims system. He then did a security check and learned that the problem had originated with a particular third-party adjuster, whose system had been breached. He contacted the company and advised they immediately shut down their system, which they did. Thankfully, we'd discovered the breach before any harm was done.

RIMS: So the damage was completely contained, thanks to the ERM protocols put in place?

Gardiner: Yes, and just in time, too. We were very fortunate in having embedded a strong culture of risk awareness across the organization. We actually created a tagline: 'Be Risk Aware.' It is ingrained into everyone's thinking. ■

Russ Banham is a Pulitzer-nominated financial journalist and best-selling author.