

SMALL BUSINESS **BIG** OPPORTUNITYSM

TRAVELERS INSTITUTE[®] | TRAVELERS^J

Philadelphia, Pennsylvania



L to R: Michael Echols, U.S. Department of Homeland Security; Joan Woodward, Travelers Institute; Matthew Gardner, AssuredPartners; and Ben Collier, The Wharton School

Philadelphia small business owners learn to manage cyber threats, natural disasters and more at The Wharton School

Philadelphia-area small-business owners converged on The Wharton School at the University of Pennsylvania to learn how to reduce risks of cyber breaches and other threats.

“We are all about trying to help small- and large-business owners and consumers, not only to survive, but to thrive,” said **Joan Woodward**, President of the Travelers Institute and Executive Vice President of Public Policy at Travelers.

As part of its *Small Business – Big Opportunity*SM symposium series, the Travelers Institute partners with professionals and entrepreneurs around the country to address small-business challenges. The Philadelphia event, “Managing Risk: Thriving After Cyber Threats, Natural Disasters and More,” was held on May 20, 2015 in collaboration with the Wharton Small Business Development Center and the Wharton Risk Management and Decision Processes Center.

Managing in a VUCA world

Delivering the keynote address, **Roch Parayre**, Fellow, Wharton Executive Education, The Wharton School; and Managing Director, Decision Strategies International, Inc., described the world as “VUCA,” an acronym for “volatile, uncertain, complex, ambiguous.” To survive in a VUCA world, Parayre said organizational leaders need to improve capabilities in six disciplines:

1. Anticipate: Monitor the markets and industry trends better than competitors
2. Challenge: Question organizational and industry assumptions
3. Interpret: Connect external data points differently to understand world ambiguity
4. Decide: Keep options open, show courage
5. Align: Rally key players, bridge differences
6. Learn: Embrace a lessons-learned culture

Cybersecurity

During the panel discussion, **Michael Echols**, Director, Joint Program Management Office, Office of Cybersecurity and Communications, U.S. Department of Homeland Security, said small businesses are “easy targets” for hackers, adding that during the past two to three years, most cyber attacks have been against small businesses. He said small businesses often do not discover the attack until it is too late. “For most small businesses, they realize that they’ve been hacked when they’re out of business.”

Echols urged audience members to proactively protect their computer system: pay for a professional firm to scan their network to understand the company’s cyber risk baseline; train employees on cyber risks and how to work safely; and develop a business continuity plan. He said cybersecurity must be “a normal function of doing business.” For more tips, Echols directed attendees to the U.S. Department of Homeland Security’s website: us-cert.gov.



Matthew Gardner, AssuredPartners, describes the steps for building a business continuity plan.

Matthew Gardner, Regional President, AssuredPartners, Inc., advised business owners to consult with their independent insurance agent to understand available cyber insurance products and the best coverage for their particular exposures.

Business continuity

Woodward pointed out that some small businesses fold after a disaster strikes. Gardner said one of the reasons may be that small businesses typically do not have the same resources as larger firms to monitor and address risks. “Big businesses have the luxury of deploying capital in an organization to manage risk. Small businesses don’t have the same luxury.”

Ben Collier, Research Fellow, Risk Management and Decision Processes Center, The Wharton School, said businesses should consider three factors to protect their operations: people’s safety, the firm’s financial soundness and business continuity. “Covering across all aspects of the risk and its effects on the firm and its employees is quite an important point here.”



Roch Parayre, The Wharton School, shares business strategies for operating in an uncertain environment.

In live audience polling, three-quarters of attendees said they did not have a business continuity plan. Gardner said a business continuity plan is valuable in helping an organization eliminate or mitigate risks, or respond to emergencies. He stressed, however, that the plan has to be reviewed regularly, as the business — and its risks — change.

More than half of the attendees indicated they had no plans in place to take measures that increase their business resiliency to natural disasters. Collier explained that a severe weather event or natural disaster could devastate a small business by disrupting “lifeline services that your business needs to survive,” such as electricity and water supplies. He said preparation requires very careful planning, because natural disasters “affect so many different aspects of a business at once.” Finally, Collier emphasized that businesses should ensure short-term business disruptions do not turn into long-term problems.

The event was the Travelers Institute’s 20th *Small Business – Big Opportunity* symposium since the series began in 2011.

To learn more about the *Small Business – Big Opportunity* symposium series, visit travelersinstitute.org/smallbusiness.