Cybersecurity – Protecting the Crown Jewels of Your Business

On Tuesday, September 26, 2017, the BABCPHL hosted a cybersecurity seminar outlining the threat landscape; presenting the mitigation responses; and discussing the complexities of the topic. Technology is both a blessing and a curse, and cyber criminals do not need visas or passports to travel between countries. Cybercrime permeates the globe, and humans are the weak link. Social engineering plays a big role in the cybercrime equation. More than 50 people from the British, French, German and Italian Chambers gathered for this dynamic discussion at the Chamber of Commerce for Greater Philadelphia.

Dr. Robert D'Ovidio, Associate Professor in the Department of Criminology and Justice Studies and an Associate Dean in the College of Arts and Sciences at Drexel University, framed and introduced the subject matter. "Online safety is a very complex problem, and it is highlighted by the diversity of the people engaged in using the very technology." Rob explained no comprehensive solution exists to protect businesses and people. Companies and individuals must have responsible environments and promote dialogue about conscientious behaviors. He set the stage for each of the panelists to discuss what constitutes a breach notification; the importance of prevention plans and education; the current risks; and the variation of laws and standards depending upon jurisdiction. To kick things off, Rob asked Larry Hershman, Partner at Black Cipher Security to lead the audience through a two minute split screen user/hacker example. Watching silently, attendees squirmed and blood pressures rose. The dramatic hacking demo showed just how sneaky a cybercriminal can be, posing as a helpful security measure update, when in fact they are anything but that. Hackers often rely on social engineering to gain access to valuable data without the compromised individual ever even knowing their information was breached. This visual example showed how easy, quick, and simple a cyberattack can be executed.

In addition to walking the audience through the hacking demo, Larry talked about the types of cyber threats that are currently out there. He discussed what can be done to mitigate risk, and how to manage complex digital forensic and data breach investigations. Mitigation includes five steps (1) determining if what happened is an incident or a breach; (2) containing it; (3) eradicating it; (4) restoring information; and (5) comprehending lessons learned. Larry also focused his discussion on personally identifiable information (PII); how it is regulated; and the latest tools and techniques available to protect data.

Dan Castle, Information Protection Director at Cigna focused on identity and access management (IAM) – ensuring the right people have the right access to the right systems for the right reasons at the right time. Dan explained IAM is a core business function, not a technical one. Entitlements are generally grouped into roles, and individuals are not granted entitlements directly, but rather through roles. These roles need to be managed as employees join, move within, or leave an organization. The challenge of being globally consistent while also regionally respective is tricky to navigate. Dan described the area of IAM as complex in nature. Much depends upon how well educated the users are; who has access to what information; and how data is stored and secured. Multi-factor authentication (MFA) has to be the way forward.

Michael Davis, Principal at Ernst & Young LLP focuses his practice on integrating cyber solutions and controls into business processes and technical operations for life sciences and health care industry clients. Michael laid the groundwork for his discussion by explaining how companies need to start by identifying what is most important to protect, and understanding how regulations and compliance mandates are addressing cyber risk. Michael stated, "People are the weakest link. Attackers, while sophisticated, are lazy. They go for the easiest targets." The financial services industry, buying and selling credit card information for example, used to be the easiest group to hit. Currently, the health care industry is a soft target.

Criminals target an individual within an organization to stealthily capture third party information, and then use very basic internet research skills to obtain additional details about a person. For example, cyber attackers steal personal information such as name, social security number, email and mailing addresses, etc. and then do a comprehensive search of social media and other sites where people willingly give away their identity, including things like children's and pet's names, to round out a person's identity. If an individual's personal healthcare record falls into the wrong hands, the aforementioned personal data isn't the only information obtained. Now medical issues, such as diseases, medications taken, etc. are in the hands of an unauthorized individual. A breach can suddenly turn into a question of life and death if a medical record is altered, and a wrong prescription is filled, and administered.

Presenters provided extremely valuable information, and painted a truly alarming picture of the threatening landscape we all traverse on a daily basis. Cybersecurity is undoubtedly a global top of mind issue affecting individuals, companies of all sizes, and every industry sector throughout the world – no one is exempt. Before inviting audience questions and answers, Rob ended the presentation portion of the seminar by asking each panelist what keeps them up at night. Michael said the speed at which everyday life is being integrated with technology. Dan said the internet of things – technology creating a trail. And Larry said the lack of awareness and understanding that everyone is a target. Every person in the room left the seminar with the clear realization that cybersecurity must be at the forefront of business practices as modern technology continues to evolve and develop.

The BABCPHL extends special thanks to event sponsors without whom this program would not have been possible: Black Cipher Security, Cigna, Ernst & Young LLP, and the Welsh Government.