Cyber Security in an Increasingly Insecure World

October 9, 2015

By Annabelle Baxter, Senior Manager, External Communications, Alliance Data

Every year, the U.S. Department of Homeland Security brands the month of October as 'Cyber Security Awareness Month.' As households purchase an increasing number of connected devices, from television to thermostats and even smart lightbulbs, cyber security awareness continues to accelerate for both corporations and consumers. We asked two of Alliance Data's Chief Information Security Officers to provide some thoughts on the subject. Mike Britton is Chief Information Security Officer for Alliance Data and Matt Fearin is Chief Information Security Officer for Epsilon/Conversant.

How has cyber security evolved during the past 5 years?

Mike Britton: Probably one of the biggest changes, in my opinion, has been the shift in view, which has gone from hoping not to incur a cyber security incident, to a new view assuming that an incident will happen at some point in time. What used to be headline grabbing news about a company getting "hacked" has morphed into a collective shrug of the shoulder and lack of surprise that yet another retailer or bank had a breach. This change in mindset has forced businesses to spend time and effort on detection and remediation, which enables more effective recovery from the outcomes of an incident.

Another big change is the move from individuals to groups and nation states taking the spotlight as perpetrators of cyber security incidents. Individuals are still out there trying bad things but the focus has shifted to actors that include Anonymous and organized crime groups. Patching systems and software, as well as good access management practices go a long way in preventing cybercrimes.

Matt Fearin: During the past 5 years, I've seen cyber security escalate in priority such that it is now a recurring theme in the Boardroom. Cybercrime has developed to such a level that it is supported by its own niche of service providers, software suppliers, financing and business models. The potential for profit and the continued success of criminal activities continues to fuel this phenomenon, and I expect it will continue to grow at a faster pace in the coming years. As a result of these changes, companies that want to protect their customers' data and their own reputation are investing in security far beyond the basic controls employed for so many years. These investments and the continued engagement of senior leadership has required security programs to mature rapidly, expand scope dramatically and move out of the dark shadows into mainstream business practices.

What are your top 2 cyber security tips for consumers?

Mike Britton: First, there needs to be an awareness that someone is always attempting to illegally gather and harvest information, and that bad guys are creative in how they accomplish that goal. The other tip would be to have a healthy dose of skepticism. Be skeptical of things that sound "too good to be true" or actions and behavior that aren't expected.

— — — — — — — — — —