MIDDLE MARKET Growth

THE OFFICIAL PUBLICATION OF ACG® Association for Corporate Growth

A New Year for Cybersecurity: What to Expect in 2016

ISRAEL MARTINEZ AND RICHARD SCHROTH, PH.D. | JANUARY 4TH, 2016

Mail Share Tweet Share Share Share

Just five years ago, terms like cyberwarfare, digital profiling, digital footprint, cyberransom and directed denial of service attacks were little known or nonexistent in the mainstream IT community, much less the general public. Today, in the wake of massive cyberbreaches at large public companies and heightened worries over the threat of cybercrime to national security, these terms have become commonplace. In such a fast-changing environment, what will 2016 bring?

We've identified 10 trends worth watching this year:

1. Mobile devices will remain the easiest path for cybercrime. This includes compromises to individuals' digital identities and to corporate networks and business operations. Mobile breaches are already in full swing, but the tools to detect them are still in their infancy. The need to integrate security across Internet, satellite and cell phone communication will be critical to business.

2. Governments, companies and organizations will react with more regulation, litigation, prosecution and settlements. Cyber concerns will prompt redundant defensive postures including more spending on cyber compliance instead of proactive investment in defense and intelligence-based security. For example, there's no evidence that being compliant with PCI (payment card industry) security standards protects companies against targeted attacks; many compromises have occurred at companies already compliant with their industry's security standards.

3. The federal government will continue to push for so-called "back-door" access to social media platforms such as Facebook, arguing it is critical to national security. Tech companies will fight back, countering in part that such measures constitute a wasted effort. Here's why: Well-organized cybercriminals have already anticipated government access to cyber encryption and have built their own applications for encrypted communication. (Consider theMujahideen Secrets encryption program for Microsoft Windows, which was offered to supporters of Al-Qaeda as a tool to protect the confidentiality of their electronic messages.)

4. A new generation of information technology positions will rapidly emerge, including chief risk officers, chief digital officers, chief information officers and chief IT security officers. Old paradigms for risk assessment will be thrown out as corporate boards require that risk teams report to the full board instead of to subcommittees. This will give cyber concerns greater weight in corporate governance.

5. Public-private information-sharing initiatives over cyberthreats will be recognized for their public relations value, but they will have little meaningful impact. Meanwhile, new back-door partnerships to share real-time threat information will become competitive advantages.

6. Insurance companies will discover they are exposed, based on how they insure cybersecurity and general, directors' and officers' liabilities with respect to new cyberthreats. The industry will create more coverage exceptions, qualifying processes and variants in its insurance policies. Industry leaders will begin to underwrite policies based on current and actionable intelligence vs. vulnerability assessments.

7. The legal system will become more adept at analyzing the complex world of cybercrime. Companies will boost proactive efforts to thwart crime, as logic in a 1932 tort case, T.J. Hooper, is applied. A writer for *CIO* magazine explains this precedent-setting case: "…two tugboats, one of which was the T.J. Hooper, were towing barges. During a storm, the barges sunk and their cargoes lost. The owners of the cargo sued the barge owners, who in turn sued the tugboat owners. They claimed that the tug operators were negligent because they failed to equip their tugs with radios that would have warned them of the bad weather." To summarize: No more passing the cyber buck.

8. Shareholders, investors, insurance companies and corporate governing bodies will discover the extent of their exposure to targeted cyberattacks. The corporate friction in behavioral ethics between denial vs. transparency regarding cyberrisk—and its potential to materially impact a company's valuation—will increase. For example, theft of intellectual property can have a far greater impact on valuation than theft of privacy information. Ethics determine whether either is reported. (In our experience, 20 percent of middle-market acquisition targets have already had their IP stolen.)

9. Startups will redefine how people identify and protect themselves as individuals. Traditional single sign-ons and passwords will become obsolete, as distinct identification variables such as voice, DNA, memory, biometric and behavior patterns evolve. A combination of these factors will make up a person's unique cyber ID, or "fingerprint." Look for companies to extend security beyond the endpoint from the device to the person.

10. The challenges we face in the dynamic world of cybersecurity will be driven by cloud technology. Increasing use of the cloud will spark significant innovation in technology strategies and risk mitigation. //

Israel Martinez *is president and CEO of* Axon Global*, a cyber counterintelligence company recognized by the Department of Homeland Security as a leader in its field. He is certified by the DHS in cyber counterterrorism and defense, and has more than 20 years of experience in enterprise risk management and governance.*

Richard Schroth, Ph.D.*, is the managing director for the* The Newport Board Group's g*lobal cyber practice where he actively leads world-class teams of cyber professionals and board-level advisers seeking to minimize cyber risk with public boards and private equity firms. Additionally, Schroth is a senior adviser to the CEO of ACG for cyber security and serves as the Executive Director of* The American University's Kogod School of Business Cyber Governance Center i*n Washington, D.C.*