Top Ten Reasons Why Cybercrime Will Continue as a Growth Industry

Money Transmitter Regulators Association

October 7, 2015
Brief Biography

• Sr. Managing Director of Cybercrime & Breach Response at PricewaterhouseCoopers LLP and currently engaged in international investigations
• Previously CEO at ZeroPoint Risk Research LLC, security executive at Dun & Bradstreet, Jefferson Wells International/Manpower Group
• Trusted Advisor to United States Secrecy Commission, created under Title IX of the Foreign Relations Authorization Act
• Cyber risk advisor to Presidential and U.S. Senate campaigns
• Advised on cybersecurity policy for a U.S. Senator
• For more than a decade worked at the National Security Institute
• Member of the American Bar Association, Criminal Justice Section
• Has appeared on ABC News, Fox News
• Author of many articles and two books on threat and risk, including “Cyber Threat! How to Manage the Growing Risk of Cyber Attacks,” Wiley, 2014
Cybersecurity is top of mind, but there’s more to be done

76% said they are more concerned about cyberthreats this year.

Detected incidents by company size*

- 2014
  - Small: 14
  - Medium: 199
  - Large: 446

* Size by number of employees: Small: Fewer than 1,000; Medium: 1,000 to 9,999; Large: 10,000 or more

www.pwc.com/us/cybercrime
Boards are concerned, but not always engaged

Security executives should not wait for the Board to ask questions about cyber-risks and cybersecurity preparedness.
These trends will shape future cybercrime surveys
Issue 1. Cyber risk transformation

• Witnessing the transformation from an IT and productivity driven era to one defined by cybersecurity risk management, defined by unrestrained and persistent theft of intellectual property, trade secrets, business proprietary competitive data

• What has served as the status quo in a world of increasingly sophisticated cyber attacks has not adequately and appropriately managed risk

• Emergent thematic strategy: determine what is necessary to protect the brand from hostile adversaries, and manage the risk of public and investor perception
Issue 2: Cyber threat diversification

- Aggressive nation-states stealing critical business information to enhance economic competitive positioning
- Transnational Organized Crime stealing financial and personal data, business information which it may sell to acquisitive nation-states
- Hacktivists disrupting operations of target entities
- Insider threat intensifying globally as nations restrict background investigations and adversaries are integrated into the workforce
**Issue 3: Diverse target range**

- Intellectual Property, Trade Secrets, Business Proprietary Information, Personal Data

- Some of the industries targeted:
  - Advanced manufacturing, materials
  - Shipping and logistics
  - Energy, pharma, bio
  - Defense, information technology
  - Healthcare, retail, financial
  - Insurers
**Issue 4: Cyber threat and risk perception**

- Historically, a concern of the CISO, CIO, etc.
- Now, this is an issue of critical importance for:
  - Board of directors
  - CEO, COO, General Counsel, Treasurer, Chief Risk Officer, Chief Privacy/Compliance Officer, Others
- Pre-2014 2030 minutes with Board Audit & Risk Committee
- Now, 90 minutes+ with full board
Issue 5: Cyber insurance

• Industry is changing, policy language subject to change
• Cyber trigger policies now offered:
  • Internet of Things:
    • Internet accessible controls enables hostile factions to gain unauthorized access into critical functions in factories and smart office buildings
    • Increased risk of loss of life, property damage, area collateral toxic contamination
  • Precedent setting case: Germany, December 2014
Issue 6: Law enforcement participation

• U.S. federal law enforcement (U.S. Attorneys, FBI, Secret Service) is reaching to companies:
  • Providing post-breach best practices
  • Working with companies pre-breach
  • Will sign binding cooperative agreements to facilitate working with companies (not binding in event of national security findings)
  • Calling law enforcement can narrow the risk gap through early threat identification leading to mitigation
  • Look for growing state and local government involvement
Issue 7: Increased regulation and accountability

• Regulations around the globe are becoming more restrictive and punitive. In the E.U., for example, in 2016 and beyond companies may be fined up to 5% of annual turnover for a data breach. The list of personal identifiers is expanding to include a wide range of information, including IP addresses.

• The U.S. S.E.C. 2011 cyber risk guidelines apply to data breaches that may or may not involve the loss of personal information but do reflect investor risk of loss. Currently defined as guidance, expect expanded regulation and accountability for registrants.
Issue 8: Potential for increased litigation

• Under evolving federal guidelines there will be more reporting or data breaches, at least by U.S. S.E.C. registrants.
• Registrants failing to adequately engage in cyber risk assessments may be subject to shareholder and investor actions.
• Supply chain and third-party vendors will face increasing scrutiny as conduits of cyber attacks as registrants come under greater scrutiny.
Issue 9: Sustained vulnerability

• Many entities remain vulnerable and susceptible to increasingly aggressive attacks.
• Even if the gap between entities and adversaries narrows, the edge always favors the aggressor.
• The reason: adversaries invest whatever is necessary to compromise system and environmental integrity. Entities must operate under budget authority and restrictions. Time is always on the side of the aggressor.
Issue 10: Economic competition

- Global economic competition fuels adversary cyber attacks.
- Think of cyber adversaries as key factors in global economic competition that are ruthless, motivated, and not generally accountable to authority, regardless of jurisdiction.
- Cyber intrusions, from data acquisition to sabotage, are cost effective measures enabling rapid competitive repositioning.
- Geopolitical realignment based on economic enablement and competition creates military, intelligence, diplomatic, cultural, and industrial imbalances.
Contact Information

MacDonnell Ulsch
Sr. Managing Director, Cybercrime & Breach Response
PricewaterhouseCoopers LLP
125 High Street, Boston, MA 02110
Mobile +1.617.634.9800 Don.Ulsch@us.pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

©2015 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers LLP which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.