High-Impact Cyber Breach Trends

Presented to:
MTRA 2014 Annual Meeting

November 6, 2104
Overview

- The Internet of Things—Breach Accelerant
- Breach Trend: Transnational Organized Crime & Military-Grade Encryption
- Nation-State: Breach expansion
- Cyber Breach Insurance: A $1B Policy
Cyber Attacks on the Rise

- Detecting cyber-attacks can be costly, inaccurate and time consuming
- Two kinds of companies:
  - Those that have been breached know it, and those that have been breached and don’t know it
- Costs are considerable and extremely variable
- Breach costs are rising as breaches become more complex
Complicating the Cyber Attack Risk

- Some attacks undetected for years
- Law enforcement overburdened
- In many organizations, executive management and the board of directors have not set their sights on the cyber threat
- Nation-state technology espionage
- Global competition
- Organized crime
- Hacktivists
- Insiders
Security often inadequate when threat scope is considered

Cyber insurance, liability insurance undergoing change

Legal, regulatory, financial and reputation risk

Risk impact measured in loss of revenue, diminished market competition, customer drift, company value
From the U.S. federal indictment:

"Liberty Reserve has emerged as one of the principal means by which cyber-criminals around the world distribute, store and launder the proceeds of their illegal activity."

--U.S. District Court

for the Southern District of New York
**Case History: How one company was impacted by Liberty Reserve**

<table>
<thead>
<tr>
<th>Personal Brand Compromise</th>
<th>Corporate Web Site Compromise</th>
<th>TOC Franchise Strategy</th>
<th>Proximity Wireless Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Third-Party Vendor Linked to Original Breach

- Extortion Demand: $1MM to Deactivate Each Website
  - Up to 100 websites

- Impact Analysis:
  - Executive Displacement
  - Deficient Security
  - Increased Federal Scrutiny
  - Possible Foreign Penetration
Don rejoined the firm in 2014 and is a Managing Director in the US Cybercrime & Breach Response practice. Working with many well known corporate brands, as well as law enforcement and the intelligence community, he has led many complex cyber breach investigations and advised executive management on breach management strategy and mitigation execution. His cases have included the compromise of regulated personal information, as well as intellectual property and trade secret theft and fraud. Don uncovered one of the largest cases of fraud and trade secret theft in US history.

He was the CEO and Chief Risk Analyst at ZeroPoint Risk Research LLC, and served in executive security and risk positions at Dun & Bradstreet/Dataquest and Manpower. Don served as Trusted Advisor to the United States Secrecy Commission, created under Title IX of the Foreign Relations Authorization Act. For more than a decade during the Cold War, he worked with the National Security Institute.

He has appeared on ABC News and Fox News as a cybercrime and breach analyst. Cited in articles, books, and academic and military studies on cybersecurity, he has lectured at Boston College and Boston University. Don is the author of two books: *Threat! Managing Risk in a Hostile World* (The IIA Research Foundation, July 2008) and *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks* (John Wiley & Sons, July 2014).
Contact Information

MacDonnell Ulsch
Managing Director
PricewaterhouseCoopers LLP
Cybercrime & Breach Response
125 High Street
Boston, Massachusetts 02110
Telephone +1.617.530.6390 Mobile +1.978.808.6526
don.ulsch@us.pwc.com