Cybersecurity Risk Management

Responding to the Inevitable Breaches

Outline

- Introduction
  - Statistics & Trends/Schemes
- Prevention, Detection & Response
- Business Impact
- Corporate Governance

General Statistics

- Over 169 million personal records were exposed in 2015, stemming from 781 publicized breaches across the financial, business, education, government and healthcare sectors.

– "ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC

- The average global cost per each lost or stolen record containing confidential and sensitive data was $154. The industry with the highest cost per stolen record was healthcare, at $363 per record.

– "Cost of Data Breach Study: Global Analysis" | IBM/ Ponemon

General Statistics

- In 2015, there were 38 percent more security incidents detected than in 2014.

– "The Global State of Information Security Survey 2016" | PWC

- The median number of days that attackers stay dormant within a network before detection is over 200.

– "Microsoft Advanced Threat Analytics" | Microsoft

- As much as 70 percent of cyberattacks use a combination of phishing and hacking techniques and involve a secondary victim.

– "2015 Data Breach Investigations Report" | Verizon

General Statistics

- Only 38 percent of global organizations claim they are prepared to handle a sophisticated cyberattack.

– "2015 Global Cybersecurity Status Report" | ISACA International

- The majority of data breach victims surveyed, 81 percent, report they had neither a system nor a managed security service in place to ensure they could self-detect data breaches, relying instead on notification from an external party. This was the case despite the fact that self-detected breaches take just 14.5 days to contain from their intrusion date, whereas breaches detected by an external party take an average of 154 days to contain.

– "2015 Trustwave Global Security Report" | Trustwave

Trends and Schemes

- Malware (viruses, worms, Tojans, ransomeware) Ransomware
- Phishing Phishing
- Zero-day Attacks (against publicly unknown vulnerabilities) Zero-Day
- Advanced Persistent Threats (APT) APT
- IoT – Internet of Things – the mobile world to include apps

Breach Prevention, Detection & Response

Prevention

- Identify what data needs protecting and back-up
- Deploy appropriate access controls
- Assess external parties
- Encypt, ENCRYPT, ***ENCRYPT***
- Build awareness within organization
- Perform periodic assessments

Detection

- Deploy systematic tools
- Create a response/escalation network
- Hiring practices(internal-temps/contractors)

Why is a Breach inevitable?

- More connectivity of devices
- The Human Factor

Business Impact

- Reputation
- Financial Impact
- Lost Productivity
- Governmental Fines (due to legal statutes)

Corporate Governance

- Ensure cyber related activities are included in corporate risk framework
- Develop an appropriate risk mitigation strategy
- Build awareness from the top-down
- Deploy competent professionals within organization
- Design and test business continuity strategies so WHEN IT HAPPENS the impact in minimized