CYBER RISK AWARENESS

MACDONNELL ULSCH
CYBER ADVISORY LLC
Smart City and Space Risk

–Disclosure: For Information Purposes Only–

This presentation is intended to provide information on a broad range of potential risk conditions and consequences based on cyber attacks that result in a breach of confidentiality, integrity or information availability. No specific industrial sector is identified or intended.

This presentation is not intended to provide legal counsel or guidance to any corporation, nonprofit entity or any U.S. or foreign government. Rather, it is a general overview reference of the types of risks that may result from cyber attacks originating externally or from insider cyber threats.

The information herein is believed to be accurate, but there is no guarantee of accuracy and certainty. Any perspective or implied opinion is that of MacDonnell Ulsch Cyber Advisory LLC and no other entity.

—Cyber Breach Risk Range—

A breach of cyber security can have unintended, long-lasting and complex operational impact on any target organization, for-profit corporation, non-profit organization or government. This presentation examines the range of risks that may result when the veil of propriety and integrity is compromised by Transnational Organized Crime, Adversary Nation States, Disgruntled Employees, and others.

Thirteen specific risk conditions are identified.

—Compromised Data Categories—

1. Intellectual Property
2. Trade Secrets
3. Proprietary Business Information, including:
   - Operational Cost Data
   - Supply/Supplier Chain Information
   - Vendor and Customer Contract Information
   - Legal and Litigation Information
   - Compensation Schedules
   - Mean Time Between Failure Component Data
   - Employee Personal Information
   - Data Breach Histories
   - Regulatory Compliance and Impairment Data
   - Other Critical Data

—Regulatory Risk—

1. REGULATORY RISK. If you or your clients are regulated by the United States Securities and Exchange commission, it is possible to have violated compliance by not reasonably forecasting your cyber risk. Disclosure of Material Risks is required. According to the U.S. S.E.C. this means disclosure of risks “to which reasonable investors would attach importance in making investment or voting decisions.” Other regulatory risks include the failure to protect personal and business information in a manner consistent with U.S. federal and foreign government requirements, U.S. state and municipality requirements, and contractual requirements.

–Legal/Litigation Risk–

2. LEGAL/LITIGATION RISK. The compromise of personal information, trade secret information, intellectual property or other types of privileged information may result in civil and even criminal litigation. These legal/litigation actions may be taken against the company or nonprofit organization, employees, executives, and/or members of the board of directors. Legal/ Litigation action may result in U.S. and foreign government sanctions, fines, regulatory impairment, and imprisonment.

—Financial Risk—

3. FINANCIAL RISK. Cyber attacks are expensive. Mondelēz International is a multinational snack company that was spun off from Kraft Foods in 2012 and is a global leader in snacks. The company's brands include iconic names such as Oreo, and Ritz. Company reportedly sustained $300 million in system damages from a cyber attack from Russia. The United Health Group cyber breach is estimated to cost the company $1.35B to $1.6B annually. Actual costs may be reflected in:

- System damage and repair and remediation
- Forensic assessment costs
- Increased insurance premiums or inability to reacquire insurance
- Fines imposed by U.S. and/or foreign regulators or other government offices
- Loss of customers/clients
- Impaired reputation
- Contract breach or violation of terms of agreement
- Loss of customer/client information, including intellectual property, trade secrets, business proprietary information and personal information
- Work stoppage, downtime due to confusion, interrupted system access, uncertainty of cyber attack consequences and short- and long-term impact
- Average cost is approximately $4.88 million per event (2024)

—Financial Risk, Continued—

Most Costly Data Breaches Are Not the Average

- NotPetya/ExPetr: $10 Billion (Mondelez International hit by this virus)
- TJX Companies: $4.5 Billion
- Epsilon: $4 Billion
- Equifax: More than $1.4 Billion
- Meta: $725 Million
- Veteran's Affairs: $500 Million
- Target: $292 Million
- Hanford Brothers: $252 Million
- Sony PlayStation Network: $171 Million
- Yahoo!: $152.5 Million

—Reputation Risk—

4. REPUTATION RISK. Reputation Risk is most often based on several critical factors. These factors include:

- How the victim entity manages the post-cyber breach event with impacted entities, including timeliness of reporting of the cyber breach event, including law enforcement authorities, as required.
- Disclosed forensic findings regarding source of the breach and how the breach occurred.
- The number of entity cyber breaches reported or discoverable.
- Remediation practices identified and implemented in the post-breach phase of each cyber breach event.
- Resulting litigation from the current or any prior cyber breach event.
- Cyber insurance coverage, including past claims, current claim, forensic findings, and pre-breach insurance disclosures.
- Financial impact on the victim company.
- Regulatory impairment: findings, fines, penalties by U.S. federal, state, municipal, and foreign country regulatory authorities.

–Customer Drift Risk–

5. Customer Drift Risk. Be prepared to experience customer drift in the event of a cyber breach. Customer loss is most often attributed to the following:

- Delayed or inadequate or inaccurate notification to customers/clients.
- Delayed or inadequate or inaccurate reporting to regulatory authorities or law enforcement, as required.
- Regulatory impairment resulting in fines and sanctions.
- Legal/Litigation against the entity resulting in financial settlements and/or criminal conviction.
- Cause of cyber breach: administrative error, employee sabotage, third-party or fourth-party vendor Service Level Agreement violation of terms, or external criminal action by an individual, criminal group or adversary government.

—Technology Risk—

6. Technology Risk. Information systems may be compromised in a cyber breach event but may not be immediately apparent. In these events the breach may result in the:

- Destruction or contamination of information system components or static or transactional data.
- Embedding of noncompliant, banned or otherwise restricted network components that violate regulatory, statutory or contractual requirements.
- Embedding of network components that silently and invisibly report back proprietary data to an adversary nation-state or transnational criminal organization.
- Creating a sound traceability methodology to ensure product origination and funding source origination can be applied to product vendors and investors to reduce the likelihood of critical proprietary data exfiltration.

–Contract Risk–

7. Contract Risk. This condition may result when a victim or targeted entity made certain commitments to a customer/client but the entity failed to meet the contract obligations on the basis of a cyber breach event. Such a condition may result in the violation of customer/client proprietary information assets, including intellectual property and other proprietary information including personal information assets. The contract may be challenged legally as a breach of contract resulting in litigation, termination, and reputation damage.

—Insurance Risk—

8. Insurance Risk. Insurance risk may result from inadequate or incorrect (intentional or unintentional) pre-breach disclosures pursuant to cyber defense readiness and security architectures articulated to the insurer. A cyber forensics examination strategy should be agreed upon with the insurer: an independent third-party cyber forensics specialist provided by the insured (at insured's cost) or by the insurer or both. To avoid avoid cyber forensics risk negotiate prior to signature authorization of the policy. Additionally, negotiate the terms of an Act of War clause that may limit the liability of the insurer, placing additional financial burden upon the insured. This issue is intrinsically linked to the cyber forensics terms and conditions.

—Employment Risk—

9. Employment Risk. In the event of a cyber breach event, an internal or external forensics impact analysis may result in the identification of linkage to an employee or contractor under the management of the entity. Forensic findings may indicate administrative error or insider sabotage, resulting in civil or criminal actions against the insider. Such action may include termination, legal remedy, loss of promotion or compensation increase or other action, such as criminal prosecution by federal, state, municipal or foreign government.

—Supply Chain Risk—

10. Supply Chain Risk. Estimates indicate that about 45% of supply chain companies have experienced a cyber breach event. This may mean that a given supplier may be unable to fulfill contractual delivery obligations, requiring customer/client entities to create backup plans to avoid downstream customer/client contractual breaches resulting in potential litigation, financial, and reputation damage. Given that much of the global supply chain includes adversary nation-states, such as the People's Republic of China, continued conflict between the United States and China over Taiwan's independence and other issues may increase the potential of strategic supply chain risk.

—Cascading Risk—

11. Cascading Risk. This typically occurs in cyber breach conditions that are complex, continuing or extremely disruptive, and where the active breach may have been undetected for months or even years. It is further complicated by entities that are not experienced, have inadequate cyber breach and legal representation, and failed to have a cyber breach blueprint for event response or fail to practice breach response periodically. These organizations may also fail to report suspect incidents to law enforcement and regulatory authorities in a timely manner out of ignorance or lack of judgment or fear of intended or accidental culpability based on inadequate budgeting and policies and procedures.

—Employee Retention Risk—

12. Employee Retention and Recruitment Risk. A cyber breach event may have many unintended consequences. Among these consequences is the post-breach inability to fund compensation increases to retain top tier employees. These employees may be targeted by competitors once a cyber breach is disclosed in the media, law enforcement, or regulators. Entities may also be unable to meet recruiting targets based on unexpected breach and associated costs. In some cases, litigation and reputation impairment may motivate employees to seek or at least be more open to recruitment to the competition.

–Threat Identification Risk –

13. Threat Identification Risk. The failure to identify specific threats will increase the risk of compromise. Threats can emanate from your competitors, disgruntled employees, rogue contractors, third-party vendors, fourth-party vendors, your supply chain, nation-state adversaries (military, intelligence, joint venture partners), transnational organized crime, independent lone wolf outsiders, domestic joint venture partners, academic partners, political partisans and activists, certain investors seeking to lower your valuation.

About the Founder: Career Highlights

N. MacDonnell Ulsch

- MacDonnell Ulsch Cyber Advisory LLC, Member and Smart City & Space Security Analyst, Specializing in China & Adversary Nation-States.
- Senior Managing Director, Cyber Incident Response, PricewaterhouseCoopers, NYC/International, Internal and External Investigations.
- Founder & CEO ZeroPoint Risk Research LLC.
- Guest Lecturer, Cyber Warfare at U.S. Military Academy at West Point & Research Fellow in Cybersecurity at Boston College, Guest Lecturer MBA Program.
- Cyber Threat Advisor to the Central Intelligence Agency, Analyst at the National Security Institute, U.S> Senate Foreign Relations Committee Briefings
- U. S. Department of the Treasury Cyber Security Task Force on Cybersecurity, Task Force Member,
- U.S. Commission on Protecting and Reducing Government Secrets, Task Force Member.
- American Bar Association, Forensics Member, Co-Chair Privacy Subcommittee.
- Author, “Cyber Threat! How to Manage the Growing Risk of Cyber Attacks,” John Wiley & Sons, Inc., 2014.
- Author “Threat! Managing Risk in a Hostile World,” Institute of Internal Auditors , 2008.
- SkyTop Media Contributing Author & Host of SLING TV Show Gray Zone Report—China.
- Near East Center for Strategic Engagement, Advisory Board.
- MPAY Inc., Board of Directors, Acquired by Tenex Capital Management, 2025.
- Vice President & Chief Analyst, Dun & Bradstreet (Investment Group)/Dataquest.
- Parliamentary Intelligence Security Forum, Member.
- The Vatican, Advisor on Technology Proliferation in Developing Nations

Contact Information

N. MacDonnell Ulsch

+1.646.957.1251 Voice & Text

Don@UlschCyberAdvisory.com

https://SmartCitiesRisk.com