Cybersecurity Due Diligence

September 2018

ALVAREZ & MARSAL

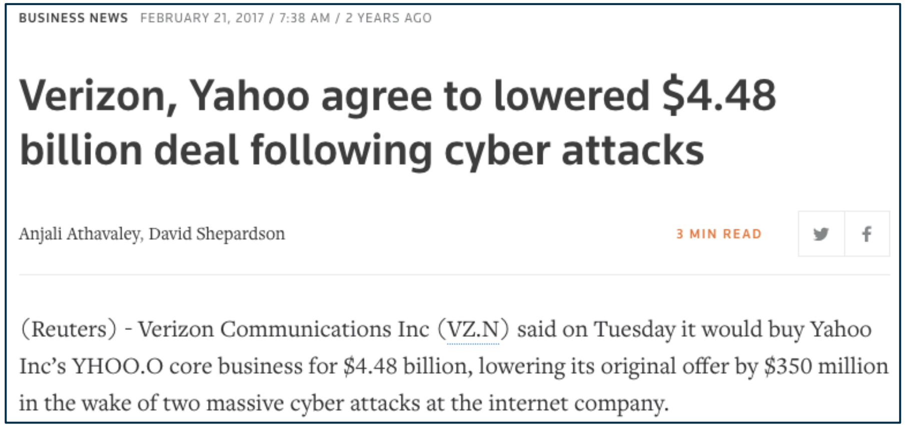
A&M

Cybersecurity Due Diligence | Why Be Concerned

Cybersecurity due diligence should be an imperative for a PE firm or other buyer that is in the process of acquiring a company.

The due diligence will assist the buyer in:

- **Understanding the cyber risk that is being acquired**
- **Developing cyber risk mitigation strategy**
- **Forecasting integration costs resulting from cybersecurity technology differences**
- **Identifying budget/resources required after acquisition**



BUSINESS NEWS FEBRUARY 21, 2017 / 7:38 AM / 2 YEARS AGO

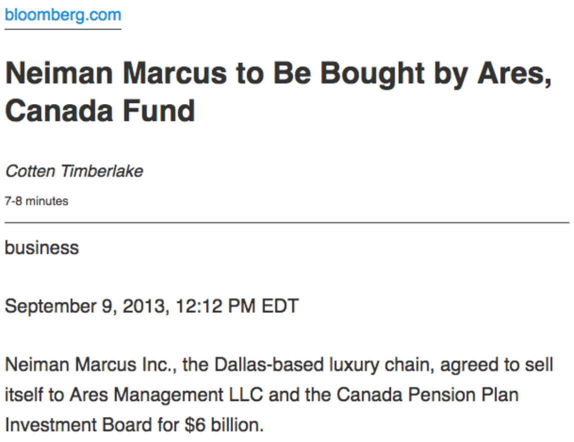
Verizon, Yahoo agree to lowered $4.48 billion deal following cyber attacks

Anjali Athavaley, David Shepardson

3 MIN READ

(Reuters) - Verizon Communications Inc (VZ.N) said on Tuesday it would buy Yahoo Inc's YHOO.O core business for $4.48 billion, lowering its original offer by $350 million in the wake of two massive cyber attacks at the internet company.

July 2013 - Malware infects Neman Marcus stores, stealing customer personal information.



bloomberg.com

Neiman Marcus to Be Bought by Ares, Canada Fund

Cotten Timberlake

7-8 minutes

business

September 9, 2013, 12:12 PM EDT

Neiman Marcus Inc., the Dallas-based luxury chain, agreed to sell itself to Ares Management LLC and the Canada Pension Plan Investment Board for $6 billion.

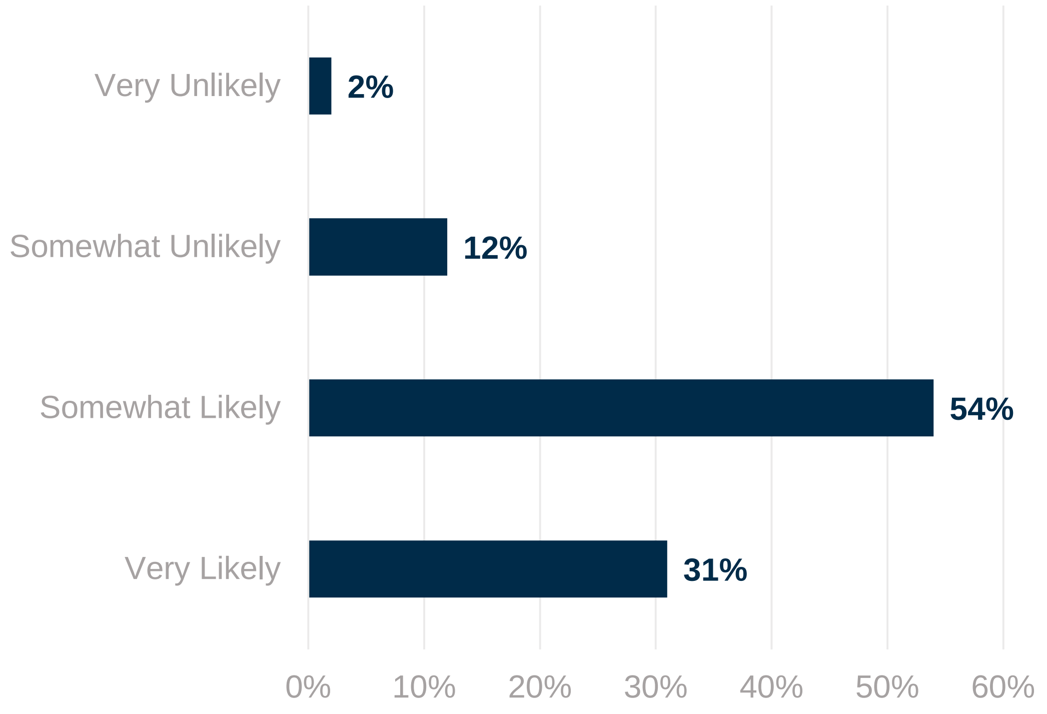
October 25, 2013 – Acquisition closed.

October 30, 2013 – Card-scraping ceased.

The Impact of Cybersecurity Threats on M&A

More than 80% of the company directors surveyed state that the discovery of major security vulnerabilities identified during an acquisition would "likely" or "very likely" affect their final decision.

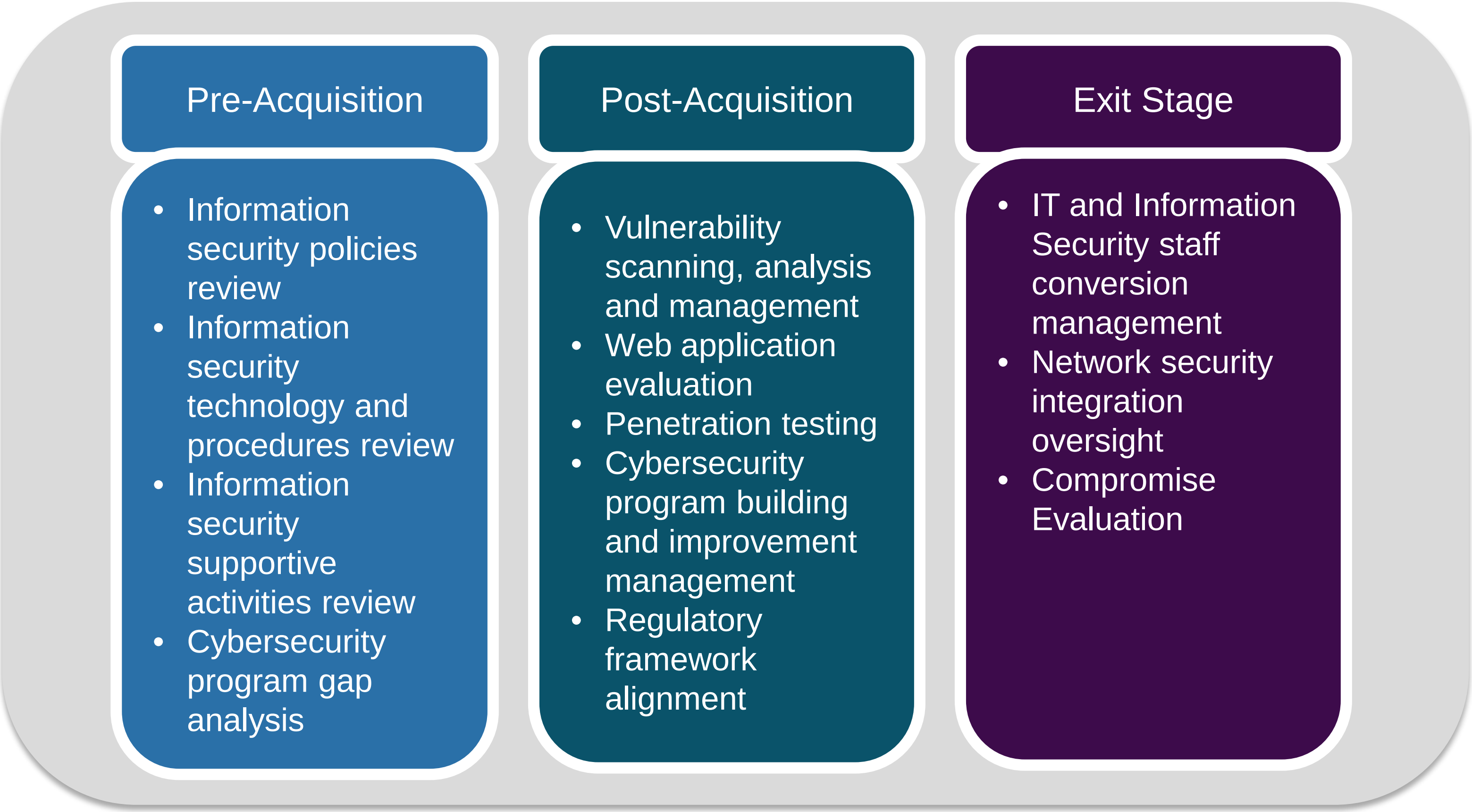
THE LIKELIHOOD OF MAJOR SECURITY VULNERABILITIES AFFECTING A MERGER OR ACQUISITION.



Note: 1) Based on the 2016 NYSE Governance Services and Veracode survey conducted on >200 public company directors and officers.

Cybersecurity Due Diligence in the Acquisition Life Cycle

It is critical that private equity firms and strategic buyers understand the cybersecurity and risk posture of every targeted company throughout the investment lifecycle. From pre-acquisition, through post-acquisition to exit, buyers should be aware of the cyber risk that a new acquisition may present.



Pre-Acquisition

- Information security policies review
- Information security technology and procedures review
- Information security supportive activities review
- Cybersecurity program gap analysis

Post-Acquisition

- Vulnerability scanning, analysis and management
- Web application evaluation
- Penetration testing
- Cybersecurity program building and improvement management
- Regulatory framework alignment

Exit Stage

- IT and Information Security staff conversion management
- Network security integration oversight
- Compromise Evaluation

Cybersecurity Due Diligence Evaluations for Private Equity

A variety of tasks are required to form an understanding of the current cybersecurity risk profile and any identified gaps in order to provide "high-level" recommendations for improvement. A cybersecurity evaluation should rely on access to personnel, documents and a completed questionnaire that will aid in developing a current state profile.

Cybersecurity Risk Evaluation Profile

- Evaluation of the company against the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) 98 subcategories that consider individual cyber risk reducing activities
- Review of cybersecurity technology and procedures for an understanding of the cybersecurity-related infrastructure currently owned and the quality of their deployment and operation
- Analysis of cybersecurity supportive activities for an understanding of the current supportive activities currently managed (e.g. SIEM and other detection tools and activities, incident response capacity, continuity operations and etc.)

Cyber Governance & Compliance

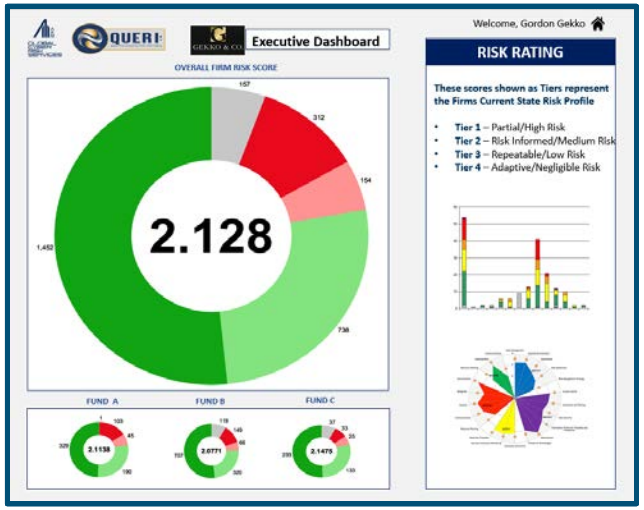
- Evaluation of compliance status (i.e. with GDPR, PCI, HIPPA or other relevant regulation)
  - Review of current policies, procedures and technology for compliance with related regulation
  - Determination of gaps identified between requirements and current compliance state
  - Identification of potential solutions (people, process, technology) that could be implemented to meet compliance mandate.

Cybersecurity Due Diligence Expectations

By performing a cyber due diligence evaluation, executives are able to better understand the risk they are assuming from a cybersecurity perspective.

Cyber Risk Evaluations allow for:

- ➢ Initial intelligence gathering to inform deeper evaluation
- ➢ Discovery of vulnerability causation
- ➢ The measurement of cybersecurity risk posture and process maturity



These scores shown as Tiers represent the Firms Current State Risk Profile

- **Tier 1** – Partial/High Risk
- **Tier 2** – Risk Informed/Medium Risk
- **Tier 3** – Repeatable/Low Risk
- **Tier 4** – Adaptive/Negligible Risk

VALUE ADDED RESULTS

- **Understand** the cybersecurity risks being acquired before the purchase.
- **Be informed** of the remediation costs of unacceptable cybersecurity risks.
- **Quantify** the known risks to positively drive down sales price.
- **Mitigate** risks to the firm during post-sale integration as a new portfolio company.
- **Reduce** operational and reputation risk of breaches and costs associated with a lack of preparation to manage breaches.
- **Protect** the portfolio with risk-informed contract requirements during acquisition.

Art Ehuan

Managing Director | Disputes and Investigations

Washington DC

Art Ehuan has a specialization in corporate and nation-state strategic cyber advisory services to include incident response, digital investigations, enterprise data protection and cyber risk assessments. Mr. Ehuan also serves as a lecturer on cyber crime/terrorism for the U.S. State Department, Diplomatic Security Service, Anti-Terrorism Assistance Program. He has lectured on cyber threats to nation-state critical infrastructure to include Advanced Persistent Threat (ATP), Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) and how to minimize cyber risk. Prior to his position as Managing Director at A&M, Art was a Director at Forward Discovery, an incident response, cyber consulting and training firm.

Mr. Ehuan served as Assistant VP and Director of the Corporate Information Security Department for USAA, a Fortune 200 financial services company. In this role, he was responsible for worldwide enterprise and strategic guidance on the protection of USAA information and established their digital forensic capability and Advanced Data Security and Incident reporting programs.

Among Mr. Ehuan's high-profile corporate positions was Deputy Chief Information Security Officer for the Northrop Grumman Corporation. He was responsible for protecting data from internal and external cyber threats, developing and managing security operations and implementing a corporate digital investigative unit. Mr. Ehuan was also a Federal Information Security Team Manager for BearingPoint (formerly KPMG Consulting), where he established information security initiatives and solutions for government and corporate organizations, as well as developing BearingPoint's corporate incident response and digital forensic services. In addition, Mr. Ehuan served as the Program Manager for Cisco Systems Information Security, where he was responsible for securing corporate networks, managing risk assessments, protecting source code and developing Cisco's worldwide digital forensic capability.

As a law enforcement officer, Mr. Ehuan has worldwide experience working on cases involving computer crimes. His extensive background conducting and managing computer intrusion and forensic investigations with the Federal Bureau of Investigation (FBI) led to his assignment as a Supervisory Special Agent assigned to the Computer Crimes Investigations Program at FBI Headquarters in Washington, D.C. In addition, he served as a Computer Analysis Response Team Certified Examiner, where he developed and conducted training for law enforcement globally. Mr. Ehuan served as a computer crime Special Agent for the Air Force Office of Special Investigations (AFOSI), where he investigated cyber crime against the network systems of the U.S. Department of Defense. Mr. Ehuan has also testified in Federal, State and Military courts in cases involving digital forensics.

Mr. Ehuan has received industry credentials including: the Certified Information Systems Security Professional (CISSP), and the Health Care Information Security Privacy Practitioner (HCISPP). He also maintains the Information Assessment Methodology (IAM) credentials with the National Security Agency (NSA).

Mr. Ehuan was previously an Adjunct Professor/Lecturer at George Washington University, Georgetown University and Duke University where he taught courses on cyber crime, incident response, digital investigations and computer forensics. He is a contributing author of Techno-Security's Guide to E-Discovery and Digital Forensics from Elsevier Publishing.