Beyond Cyber Liability Risk
Edward Chang
Travelers Indemnity Co.
Disclaimer

- This presentation is for general informational purposes only. This presentation does not amend, or otherwise affect, the terms, conditions or coverages of any insurance policy issued by Travelers. This presentation is not a representation that coverage does or does not exist for any particular claim or loss under any insurance policy. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy provisions, and any applicable law.

- This presentation is not intended as legal advice. A company should always seek the advice of a qualified attorney when evaluating legal or statutory considerations.

- This presentation is not intended as insurance advice. A company should always seek the advice of a qualified insurance agent or broker when considering their insurance coverage.
Cyber risk is constantly evolving
96% of businesses use one or more cloud services.

- 21% use public clouds
- 4% use private clouds
- 71% use both

Cloud challenge:
77% of respondents consider cloud security to be challenging.

Source: RightScale®, "2018 State of the Cloud Report"
Evolution of computing leads to the cloud
Types of cloud services

- **Software as a Service**
  - Use it
    - Access to user applications
    - E.g., accounting system

- **Platform as a Service**
  - Build on it
    - Development environment
    - E.g., machine learning tools

- **Infrastructure as a Service**
  - Migrate to it
    - Raw computer resources
    - E.g., storage or processing
Are cloud services secure?

- GREATER focus on security
- AVAILABLE resources and expertise
- EASIER maintenance
- FEWER vulnerabilities
- AUDIT requirements
One fish, two fish, old fish, new phish...
What is multifactor authentication?

1. **SOMETHING YOU KNOW**
   - username
   - ******

2. **SOMETHING YOU HAVE**
   - [Image of a mobile phone with a code]
   - [Image of a USB drive]
   - [Image of a fingerprint]
   - 962561

3. **SOMETHING YOU ARE**
   - [Image of a fingerprint with a checkmark]
Top security issues in the cloud

1. Data breach
   - 7% of cloud storage reviewed allowed unrestricted access
   - 35% were unencrypted

2. Insecure APIs
   - Unencrypted APIs were allowed unrestricted access

3. Weak access management
   - 27% of companies have user accounts that are potentially compromised
   - 25% of companies have been victims of cryptojacking

Source: McAfee™, “Two Easy Steps to Prevent AWS S3 Leaks”
Source: RedLock, “Cloud Security Trends,” May 2018
Credential stuffing and other cloud vulnerabilities

Company A
“On prem”
Credential stuffing and other cloud vulnerabilities
Cloud security

- Develop a cloud strategy
  - Prevent shadow IT
  - Manage 3rd and 4th-party vendors
- Understand security responsibilities
- Properly configure cloud services
  - Access controls
  - Encryption
  - Logging
- Test and audit cloud security
Vendor (supply chain) vulnerabilities

62% of financial institutions do not hold their vendors to the same cyber security standards they use\(^1\)

78% increase in supply chain attacks,\(^2\) which can lead to:

- Network compromise
- “Formjacking”
- Trojanized updates
- System outages

\(^1\) Source: Accenture, From Insecurity to Resiliency, 2018.
IRL: Compromised payment portals

Pompano Beach warned nearly 4,000 residents of data breach

City of Bakersfield announces cyber hack in online payment system

Security Issues with Online Water Bill Payment System
Ransomware update

Malware incidents involving ransomware

- 12% Increase in ransomware attacks on businesses
- $6.7M In ransom collected by “Boss Spider”
- 64% Of cyber victims are re-targeted by hackers


The Daily Tar Heel

What’s going on with the internet virus in Orange County?
How are alerts handled?

- 44% not investigated
- 9% not remediated
- 10% remediated
- 37% unsubstantiated

Source: Cisco Security Research, Annual Cybersecurity Report, 2018
Do you have the controls you need?

**Fundamental controls:**
- User education & training
- Patch management
- Multi-factor authentication
- Incident response
- Secure backups

**Advanced controls:**
- Sandboxing
- Virtualization
- User behavior analytics
- Threat hunting
- Secure, strategic cloud
Privacy-related legal developments

**State Laws**
- All 50 states now have laws addressing data privacy events

**Federal Law**
- SEC joins other federal regulators in privacy enforcement

**And...**
- Significant settlements in breach-related securities litigation
- PCI publishes software security standards
The new wave of privacy laws

- Effective as of May 25, 2018
- $57M fine against Google by French DPA
- Other active DPAs include UK, Germany, Austria, and Portugal

- Effective as of January 1, 2019
- Focus on data subject rights: notice, opt-out, data portability, etc.
- Provides for statutory damages in the event of a breach
**FFIEC guidance on cyber insurance**

- Involve multiple stakeholders in the cyber insurance decision
- Perform proper due diligence to understand available cyber insurance coverage
- Evaluate cyber insurance in the annual insurance review and budgeting process

“[C]yber insurance may be an effective tool for mitigating financial risk associated with cyber incidents.”
Cyber insurance: Helping to manage evolving risks

First party coverages
- Crisis management
- Remediation and notification
- Fraud
  - Computer fraud
  - Funds transfer fraud
  - Social engineering fraud
- Extortion (ransomware)
- Business interruption
  - Contingent BI
  - System failure
  - Reputational harm

Third party coverages
- Network and information security liability
- Content and media liability
- Regulatory liability
Thank you!