"Cyber is the most dangerous weapon in the world – politically, economically and militarily."[1]

-- Bob Gates, Former Defense Secretary and Vice Chairman of the JPMorgan International Council

Four main topics will drive this panel discussion. First, we will highlight the risks—exposures, attack types and vectors. Second, we will discuss typical and add-on cyber insurance coverages. Third, we will highlight trends in attacks and coverages and finally, we will spend some time discussing best practices to ensure insurability and ensure the most coverage for the least premium.

1. What Is The Nature Of These Risks?

Two broad categories of risk are generally covered by cyber insurance: cyber and privacy. Cyber risks include attacks, such as ransomware, business email compromise, denial of service attacks, data destruction and the like. Privacy risks include data breach and unintentional violation of privacy laws or regulations (where allowed). Privacy risks have expanded rapidly due to the adoption of new comprehensive privacy laws in six states, and especially litigation involving the California Consumer Privacy Act, which includes a private right of action. The Illinois and, recently, the New York City biometric privacy laws have inspired numerous class actions.

During 2022, the Internet Crime Complaint Center (IC3), received 800,944 complaints. Reported losses reported exceed $10.3 billion.[2] This number represents a 5% decrease in reports and a 49% increase in losses.

According to the Cybersecurity and Infrastructure Security Agency (CISA), 47% of American adults have had their personal information exposed on the Internet[3]. Data breaches are one of the key risks presented by cyber criminals. Businesses can lose valuable work product, confidential information, trade secrets that might be crippling to the company, and generate claims from clients, employees and others. "Ransomware" attackers hold this critical data for "ransom" until the business pays the ransom, typically in difficult to trace cryptocurrency, to accounts that they quickly drain and close.

Cyber Insurance Products

The significant increase in the costs of cyberattacks has spurred the growth of the cyber insurance market. Gone are the days of a basic Commercial General Liability ("CGL") policy

[1] Matt Egan, *"Cyber is the most dangerous weapon in the world," JPMorgan council warns* (Dec. 16, 2021), https://www.cnn.com/2021/12/16/business/cyber-security-hacking-jpmorgan/index.html.

[2] FBI, "*Internet Crime Complaint Center Releases 2022 Statistics*," (March 22,2023), https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics .

[3] CISA, "*The Facts*," https://www.cisa.gov/be-cyber-smart/facts.

providing all the coverage the average business needs. Cases, such as *Mondolez v Zurich*[4] spawned exclusions specifically directed at cyber and privacy events, thus encouraging more commercial and private entities to seek risk transfer via stand-alone and add-on cyber insurance policies. Cyber insurance is no longer a handy add-on, but a necessity.

In sharp contrast to property insurance covering damage to a home, for example, cyber insurance is a relatively new phenomenon. Insurers have less historical data on which to shape the language of cyber policies, and determine prices, than they do with standard property policies. The nature of cyber, and increasingly privacy, is that the risks evolve swiftly, making both data and policy language in a constant state of flux.

One of the key challenges in this area is, and will be, the constancy of technological changes. To continue the property insurance comparison, historical data on home fire claims is helpful, because the basics of homes, and the fires that destroy them, have not changed all that much in the past two hundred years. Cyber claims change far more substantially due to the evolving risks, changing policy terms and the legal landscape. In the cyber realm, both the "homes" and the "fires" that attack them are a moving target. There simply is no set of reliable data upon which models, pricing and policies can rely.

At the present time, and while coverages vary, many of the cyber liability policies on the market are designed to cover:

- Defense and liability costs which may arise from data breaches or claims made by company clients or others who sustain damages due to the inoperability of policyholder computer systems;
- The costs of negotiation with threat actors, including extortionists;
- Ransom payments;
- Business interruption and lost income to the policyholder due to computer system outages or interruptions from cyberattacks;
- Regulatory fines from state and federal agencies;
- Notification expenses to affected individuals in the event of a data breach or compromise;
- Credit monitoring services for individuals whose personal information is compromised;
- Public relations expenses;
- Data restoration;
- System remediation;
- IT forensics.

[4] Adam B. Schniderman, "*Prove it! Judging the Hostile-Warlike-Action Exclusion in Cyber-Insurance Policies*," "Yale Law Journal, (Oct. 19, 2019), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.yalelawjournal.org/pdf/Shniderman_ProveIt_46vzsvqt.pdf

Additional coverages may include:

- Fraudulent funds transfer;
- Computer fraud;
- Reputational harm coverage, providing indemnity for the continuing impact of brand reputation damage;
- Bricking, which provides coverage for the replacement cost of technology equipment rendered useless by a malware attack;
- Betterment.

Many of the current standard policies do not provide coverage for:

- Loss of value due to theft of intellectual property;
- Potential future profits; or
- Bodily injury and/or property damage.

Due to the significant increase in attacks and dollar losses, a market for personal cyber insurance covering individuals has emerged, often as an add-on to a homeowners' insurance policy. This market is truly in its infancy. Insurers offering personal cyber insurance typically offer coverage related to:

- Restoration of a computer, and removal of a computer virus;
- Cyberbullying (online harassment, including expenses following cyberbullying, such as counseling, relocation, security software);
- Cyber extortion (assistance from experts, consultation and negotiation, reimbursement for amount paid);
- Fraud (losses from identity theft, social engineering, unauthorized banking, and other types of fraud);
- Home systems attack (restoration of smart devices following an attack).

Prevention Tips and Strategies

While it is difficult to hit the moving cyber target, some best practices have begun to develop in this emerging field:

1. **Multi-factor authentication (MFA)**, was once considered an unnecessary annoyance by many technology users. It is now a basic, critical minimum for any cybersecurity

system. Extra layers of security exponentially increase the difficulty for cyber attackers. It is estimated that MFA can block as many as 99.9% of account compromise attacks.[5]

2. **Employee Training**. No MFA can protect against an untrained employee who clicks on the wrong phishing email, unwittingly granting cyberattackers access to their employer's system.

3. **Encryption of sensitive data and personally identifiable information** both at rest and in transit provides a critical layer of protection. This is true not only because hackers cannot read encrypted data, but because many data breach statutes exempt encrypted data breaches from liability.

4. **Implementation of a strong password control policy** adds protection. In fact, some underwriters will not write a cyber insurance policy if password best practices are not followed. Strong passwords are typically *at least* 8 characters long, do not contain words found in the dictionary, include upper and lower case letters, numbers, and one or more special characters or symbols.

5. **Regular penetration testing** of a cyber system can serve to proactively identify weaknesses and allow for correction before a cyberattack. There are a growing number of service providers who can be hired to test the quality of one's cybersecurity system. In some cases, insurers are testing policyholder or applicant's systems on their own as part of the underwriting process.

6. **Keeping software up to date** and utilizing appropriate security patches as they are made available can keep a system safe. Patches are typically made available when a vulnerability is detected, so utilization and frequent updating keep systems as healthy as possible.

7. **Proactively backing up data** is a vital step in mitigating any losses should a cyberattack take place. In the event of a cyberattack, having an adequate back up is the difference between a hiccup in operations and a catastrophic event. Ideally, redundant backups- in the cloud as well as air gapped (not connected to the Internet) should be regularly made, tested and archived, as threat actors often are in a system for months before launching an attack.

8. **Formation of a breach response plan** is essential. The timing of a response to a cyberattack can make a critical difference in preventing or mitigating it. Certainly loss of access to a computer system can be crippling. Preparation and contingency plans can make all the difference when systems are down or inaccessible. ENSURE THAT YOU HAVE A HARD COPY OF YOUR INCIDENT RESPONSE PLAN. Do not rely on a plan that resides on your computer system, as you likely will not be able to access it in the event of an attack.

---

[5] Melanie Maynes, *One simple action you can take to prevent 99.9 percent of attacks on your accounts*, Microsoft Security Blog (August 20, 2019), https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/.

Recent Trends And Impact On The Insurance Industry

While ransomware seems to have hit its height during the pandemic, attacks seem to be declining and have become less lucrative, as fewer victims pay ransom. Threat actors have recently moved away from encryption attacks, opting instead to exfiltrate (steal) data and use that as the basis for extortion, demanding payment in return for a promise to refrain from publishing the data on the dark web and deleting it following payment. Given the nature of the transaction, victims have chosen to decline payments. This is due partly to the recoil at paying criminals, who are inherently untrustworthy, and to better backups and security practices.

Increasingly, people work from home and utilize remote computing. Whereas this practice may have been hastily deployed during the COVID pandemic, better practices have reduced exposure. Still, work from home and "bring your own device" practices have created exposures that did not previously exist.

New state, federal, and international privacy laws are being implemented that significantly impact cybersecurity and the cyber insurance industry. For example, the California Consumer Protection Act ("CCPA"), went into effect first, in 2020,[6] with six states following the lead, adopting comprehensive privacy laws. That said, to date, only the CCPA provides for a private cause of action.

Cyber insurance premiums were generally on the rise until recently, when the market started to stabilize. Increased stability seems to be due to underwriting being more stringent, implementation of exclusions and requiring more system controls. Policies and systems that used to help secure a premium discount (like MFA) are now considered basic cybersecurity tools that are often required as a prerequisite to coverage.

[6] Cal. Civ. Code § 1798.100, *et seq.*