Insurance Coverage Against Cyberattacks: Emerging Products, Trends, Developments, and Strategies

By
Alex J. Brown, Shapiro Sher Guinot & Sandler
Dan Burke, Woodruff Sawyer
Monique Ferraro, Hartford Steam Boiler Inspection and Insurance

"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

Cyberattacks have more than doubled in the past four years.[2] The recent COVID-19 driven increase in remote work has only exacerbated the cybercrime risks. Cybercriminals are continuously modifying and improving their tactics to keep up with new and changing technologies. The FBI's Internet Crime Complaint Center ("IC3") reported a 69% increase from 2019 to 2020 in cybercrime complaints, with losses exceeding $4.1 billion.[3] Insurance coverage against these attacks is now a necessity.

In this panel discussion, we will discuss three main topics. First, we will highlight some recent examples of high profile cyberattacks to illustrate the nature of the risks. Second, we will discuss insurance industry responses to these risks through new insurance policy forms and the changes in insurance underwriting that have come with those new coverages. Finally, we will spend some time discussing best practices, and predictions for the future.

1. High Profile Cyberattacks – What Is The Nature Of These Risks?

The **Colonial Pipeline** ransomware attack highlights the need for cybersecurity protecting critical business systems, employee training, and the devastation that can occur when appropriate protections are not in place.

Colonial Pipeline is a petroleum pipeline business that supplies gasoline to the majority of the Eastern Seaboard. On May 7, 2021, a Colonial employee discovered a ransom note from a cyberattacker demanding millions worth of cryptocurrency. Just over an hour later, the attackers shut down the entire Pipeline – for the first time in its 57-year history.

The immediate impact was devastating. Gas shortages caused skyrocketing prices and huge lines at the pump. Even though Colonial paid the hackers approximately $4.4 million in cryptocurrency, it took five days for the company to resume service.

An investigation revealed that the attackers gained entry to Colonial's network through a virtual private network (VPN) account. VPN accounts allow employees remote access to a company's computer network. The hackers exploited what some consider a weakness in Colonial's VPN – the VPN did not require multifactor authentication ("MFA") to gain access.

---

[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] *Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats*, 117th Cong., House Committee on Oversight and Reform (Nov. 12, 2021) (meeting notes).

[3] *Internet Crime Report 2020*, Federal Bureau of Investigation Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

MFA-protected networks require an individual attempting to gain access to a system to clear more than one hurdle to achieve entry. By way of example, an MFA-protected system might require a user to type in a password (factor one), and then respond to a prompt on their cell phone (factor two) to gain access.

The FBI was ultimately able to recover only about half of the ransom paid, approximately $2.3 million.

The **U.S. Government Office of Personnel Management ("OPM")** cyberattack was one of the most high-profile and far-reaching successful cyberattacks on the U.S. government to date. Even today, the precise timeline of the security breach is unclear, but it appears the attack began in November 2013.

Government officials did not realize OPM had been hacked until four months later, in March 2014. OPM initially believed that the data of approximately 4 million personnel were breached. It was later discovered that 21.5 million individuals were affected. Sensitive confidential background information, including social security numbers, personnel records, and fingerprint data were captured by the hackers.

Data breaches of this type are one of the key risks presented by cyberattackers. 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 untraceable digital currency, to untraceable (or difficult to trace) accounts.

Just recently (at the time of submission of these materials in December 2021), **Kronos**, a human resources management company, suffered a ransomware attack that may keep its systems offline for weeks. We will know more by the time of our February 2022 meeting.

Affected Kronos customers come from all over the United States, including the New York Metropolitan Authority, public workers in Honolulu, and the city of Cleveland. Affected employers were required to bypass Kronos functions, and for the first time in years, manually track hours and issue paper paychecks.

At this time, experts have not yet determined how Kronos was hacked, nor can the full impact be predicted. It is reasonable to expect Kronos clients to make claims against Kronos for: the time and money clients invested in setting up and operating new manual employee pay systems to replace their deactivated Kronos systems and damages arising from the release or compromise of confidential personal or corporate information on the Kronos systems, among other potential damage claims.

Cyber Insurance Products

The significant increase in cyberattacks in recent years has necessitated the equally exponential growth of the cyber insurance market. Gone are the days of a basic Commercial General Liability ("CGL") policy providing all the coverage the average business needs. 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. Over time, as insurers collect increasing amounts of claims data, carriers should be able to more accurately price risks and expertly craft policy terms.

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 might be expected to change far more substantially in the next twenty years than property claims have changed in the past two centuries. In the cyber realm, both the "homes" and the "fires" that attack them are constantly modified with by new technologies.

There is also a geographical limitation to fire claims. One need only investigate a finite amount of property, in a finite area, to protect against future house fires or to determine a fire's origin after it occurs. The fact that many cyberattacks can be launched from unknown places, by unknown individuals, increases the complexity of evaluating, underwriting and covering them.

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

- Defense and liability costs which may arise from, by way of example: 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 cyberattackers, including ransomware attackers;
- Ransom payments and other payments to perpetrators.
- Business interruption and lost income to the policyholder business 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; and

- IT forensics.

Even at this early stage, creative insurers have developed cyber policy enhancements, which include:

- More expansive 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; and
- Coverages that address the unique challenges of fraudulent funds transfers arising from a cyberattack.

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

- Loss of value due to theft of intellectual property;
- Improvement to technology systems after a cyber event;
- Potential future profits; or
- Bodily injury and/or property damage.

Due to the significant increase in cyberattacks over the past several years, an even newer 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 coverage seem to be offering 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).

Some Best Practices To Prevent Cyberattacks

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

1. **MFA**, discussed above, 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.[4]

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** provides a critical extra layer of protection. Data encryption adds an extra barrier that may be the difference in protecting confidential company information and secrets. Even in the event attackers break the encryption, the policyholder's investment in encryption may provide the company much needed liability protection in data breach or other suits. The encryption key must also be kept secure and there should be tight controls over who has access to such material.

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 can be the difference between a hiccup in operations and a catastrophic event. To protect against floods, fires or other property damage events, off-site back-ups are helpful.

8. **Formation of a breach response plan** is also helpful. 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.

---

[4] 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

Ransomware is not new, but its growth now makes it a "multi-billion dollar criminal industry."[5] If ransomware trends stay on track, 2021 ransom-related transactions "will be higher than the previous 10 years combined."[6] The ransomware trend has only been exacerbated through the improvement of encryption technology and advent of cryptocurrency, which provide ransomware criminals security and anonymity.[7] Ransomware attackers are constantly evolving and trying new tactics, often leaving those impacted with no choice but to pay the ransom demanded.

Although ransom demands and payments can vary greatly, in 2020, the average ransom paid by a mid-size organization was $170,404.[8] The average cost for recovery from a ransomware attack, including downtime, people time, device cost, network cost, lost opportunity, ransom, and more was $1.85 million.[9]

The COVID pandemic has also exposed the vulnerabilities of many businesses that were not adequately prepared to transition to a largely remote work environment. Businesses were forced to rapidly expand remote capabilities, and allow employees to work from home. Many were simply ill-prepared. Remote workers were often using less secure home networks and personal devices, giving hackers a better chance at access. Cyber attackers took advantage of the pandemic, hacking video conferencing tools, personal networks, and increased phishing attempts. Additionally, with employees largely working from home, some may have experienced delays in discovering and responding to attacks. As the world gets used to this "new normal" of a more remote work environment, cyber attackers' tactics are likely to increase in volume and sophistication.

New state, federal, and international privacy laws are being implemented that significantly impact cybersecurity and the cyber insurance industry. For example, in January 2020, the California Consumer Protection Act ("CCPA"), one of the nation's toughest consumer privacy laws, went into effect.[10] The CCPA imposes significant requirements on businesses with regard to their data security practices, third-party sharing, and disclosure of collection practices. Business compliance can be expensive and violation of the law can be costly. Cyber insurers are paying close attention to these new laws and regulations and adjusting their underwriting practices and premiums accordingly.

---

[5] *See supra*, fn. 2.
[6] *Id.*
[7] Dan Burke and Scott Goettelman, *Ransomware Attacks and Your Cyber Insurance: A Complete Action Plan*, Woodruff Sawyer (Feb. 20, 2020), https://woodruffsawyer.com/cyber-liability/ransomware-cyber-insurance-action-plan/.
[8] *The State of Ransomware 2021*, Sophos, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.
[9] *Id.*
[10] Cal. Civ. Code § 1798.100, *et seq.*

Cyber insurance premiums are generally on the rise due to the significant uptick in cyberattacks, as well as increased government scrutiny. Underwriters are being more proactive, asking more questions, 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.