"Cyber Insurance": Coverage, Trends, Developments and Strategies

Alex J. Brown, Shapiro Sher Guinot & Sandler, P.A.

David Anderson, McGill and Partners

Monique Ferraro, Hartford Steam Boiler Inspection and Insurance

Discussion topics



- The Risks
- Coverage
 - What is Cyber Insurance and What Does it Cover?
- Trends
 - Claims
 - Underwriting
- Developments
- Strategies
 - Ensuring Insurability

Types of risk "Cyber Insurance" may cover



- Cyber
 - Ransomware
 - Business email compromise
 - Denial of service
- Privacy
 - Data breach
 - Biometric
 - International, state privacy regulation (unintentional violations)
 - Website tracking
 - Privacy notices
- To get the right coverages, the broker needs to know about your business and needs

Nature of the risk- Cyber



Reported Internet crimes going down (-5% in 2022) while losses going up (+49%) (IC3) Increase in nation state sponsored attacks Critical infrastructure increasingly targeted, particularly in EU by Russia Cryptocurrency and tech industry may be affecting lower rate of attacks- different focus –Shift (small) from \$ to geopolitical advantage

Source: Pixabay

Nature of the risk- Privacy



 Many claims and losses entering the market are long tail privacy liability claims including:

- –Unlawful or unauthorized collection claims
- -Violations of privacy due to cookies or web tracking or web (or actual) surveillance
- The intersectionality of professional and privacy liability claims continue to put pressure on insurers and policyholders
 Technology liability claims
 Professional liability claims
 Claims for bodily injury and/or property damage arising out of a cyber event

What does commercial cyber insurance typically cover?



- Defense and liability costs.
- Negotiation with cyber attackers.
- Ransom payments.
- Business interruption and lost income.
- Regulatory fines from state and federal agencies.
- Notification expenses to affected individuals.
- Credit monitoring services for affected individuals.
- Public relations expenses.
- Data restoration.
- IT forensics.

Other Coverages Available



What does business cyber insurance typically <u>not</u> cover?

X	Loss of value due to theft of intellectual property.	
X	Improvement to technology systems after a cyber event.	 Unless betterment is included or unplanned obsolescence language is embedded.
X	Potential future profits.	
X	Bodily injury and/or property damage.	Unless coverage is added back in.
X	Regulatory fines and penalties where prohibited by law	 Most favorable venue and choice of law provisions are KEY here
X	Intentional acts or unlawful collection	With varying control group limiters
X	Indirect or consequential loss.	
X	Theft of Money or Securities (including crypto)	

Personal cyber insurance



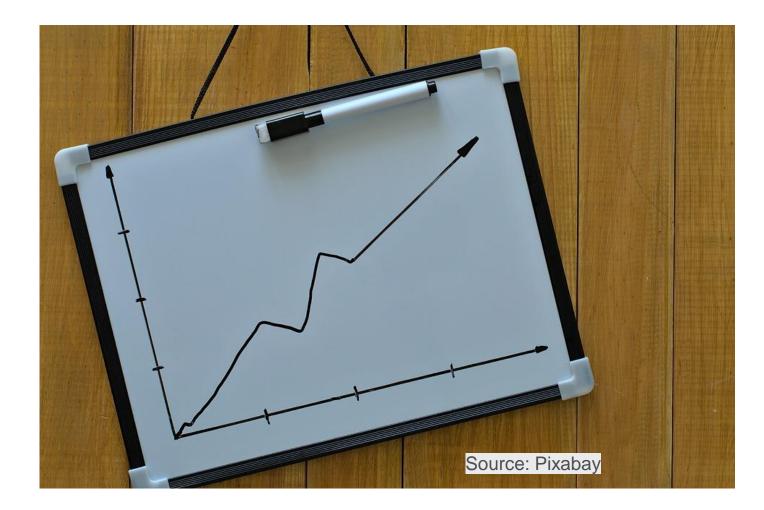
- Market is VERY new.
- Coverage often offered related to:
 - Restoration of computer and removal of virus.
 - Cyberbullying.
 - Cyber extortion.
 - Fraud and credit file abuse (identity theft)
 - Home systems attack.

Coverage trends



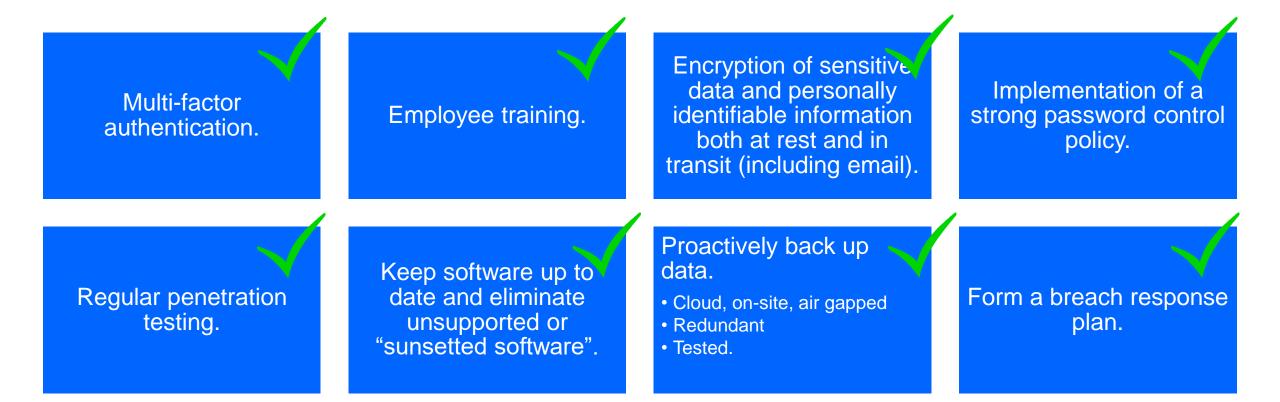
- Limits and deductible choices...
- Expanded privacy cover
- Biometrics
- IoT/OT
- War and State Sponsored Attacks exclusions
- Additional exclusions for
 - failure to patch
 - widespread event exclusions;
 - systemic risk (contingent business interruption)
 - unlawful/unsavory data practices exclusions

Risk and claims trends



- Ransomware was on the rise but seems to be leveling off
 - Extortion without encryption
- Increased challenges due to WFH and/or BYOD.
- New state, federal and international privacy laws.
- Premiums leveling/softening.
- More proactive underwriters
 - Use of tools such as "outside-in" and "inside-out" vulnerability scans.
- Artificial intelligence (AI) assisted attacks

Prevention strategies



Tips for securing the best coverages at the best price

Do not ad lib on the application

- Have your IT, law department and risk management participate in the application process
- Don't sign an application without knowing what it says

Telling your story to the marketplace: Proactive, Rehearsed, Aware, Humility, Pragmatism

- Don't ever tell an underwriter "we're not a target" or "we're totally untouchable" - instead help your underwriters understand how WELL PREPARED your organization is for when the INEVITABLE attack happens.
- Underwriters are no longer pricing risk based on how well they think you can keep attackers OUT; they are pricing risk based on how well you can RECOVER.

Questions?

