ITA

CYBER LIABILITY

AGENDA

2025 TRENDS

RECENT CLAIMS

UNDERWRITER CONCERNS

LESSONS LEARNED

CYBER COMPONENTS

GOOD NEWS

2025 CYBER MARKET

WHEN THERE'S A CLAIM

WHAT IS CYBER LIABILITY?

BEST PRACTICES

COMMON MISCONCEPTIONS

Q&A

2025 CYBER TRENDS

01

Cybercrime costs continue to rise

Worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025, emphasizing the need for enhanced cybersecurity measures (Statista).

02

Vishing attack frequency explodes

Voice phishing (vishing) attacks, where adversaries call victims to amplify their activities with persuasive social engineering techniques, saw explosive growth — up 442%

03

Small businesses struggle with resiliency

35% of smaller organizations struggle with cyber resilience while large organizations show steady progress at 7%

04

Human error drives losses

68% of cyber security breaches involved a human element in 2024 and 88% of cyber security breaches are cause by human error (Verizon, Stanford).

05

Phishing incidents are most common

Phishing attacks account for more than 80% of all reported security incidents and $17,700 is lost every minute due to a phishing attack (CSO Online).

06

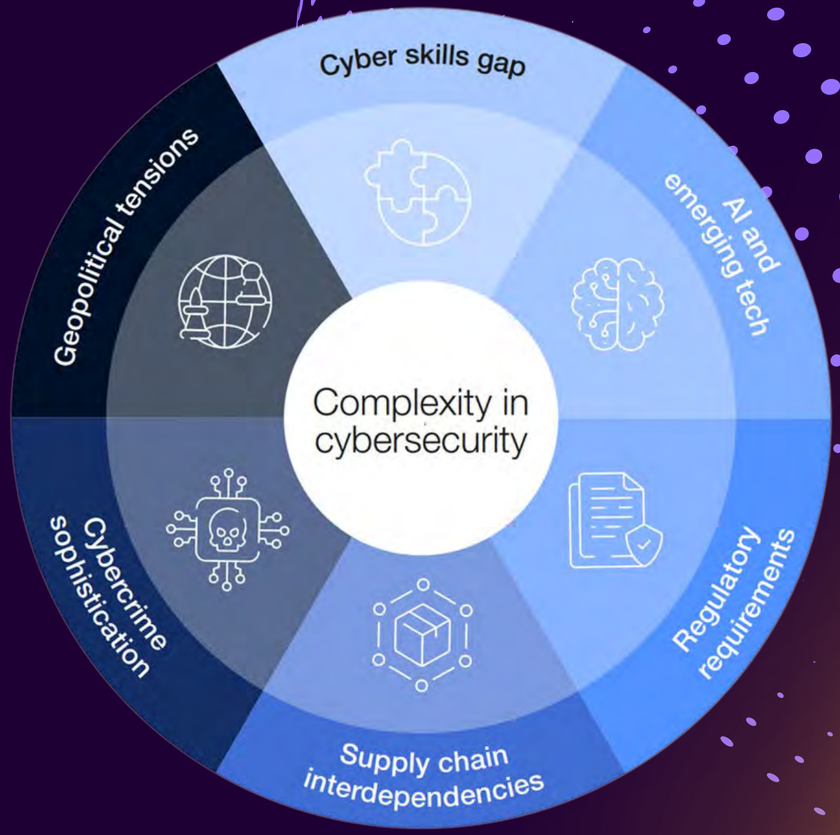
We are un -prepared

56% of American do not know what steps to take in response to a cyber security incident (Varonis).

COMPONENTS OF CYBER SECURITY

CYBERCIME IS INCREASING WITH DRIVERS INCLUDING GEOPOLITICAL TENSIONS, AI & EMERGING TECH, AND SOPHISTICATION OF THREAT ACTORS

HIGH NET WORTH AND ULTRA NET WORTH CLIENTS ARE PRIMIER TARGETS. THOSE ADVISING THESE FAMILIES ARE OFTEN THE FIRST TARGET OF THREAT ACTORS



COMMON MISCONCEPTIONS

AI can automate the process of vulnerability scanning and assessment, identifying weaknesses in systems and applications before they can be exploited.

USING A THIRD PARTY VENDOR DOES NOT TRANSFER ALL EXPOSURE

A data breach can occur while data is in transit, not only in the portal or platform used to access it

NO PROTECTED INFORMATION ON YOUR DEVICE ISN'T FOOLPROOF

Hackers have been able to intercept data in real time, skimming passwords, data, and other sensitive information

CLOUD PROVIDERS ARE NOT IMMUNE TO RISK

There is inherent vulnerability in storing data in the cloud. Cloud providers are often targeted by high tech criminals

RECENT CLAIM EXAMPLE

Trustees are often targets due to having care and control of significant assets

01

Email Compromise

Threat actors watch emails between trustee and client regarging consistent monthly distribution

02

Attack initiated at busy time of year

Around the holidays, a routine distribution was initiated. A request came to change the wire instructions. The back office vendor did verify via call-back. The bank verified directly with the trustee, rather than the back office

03

Wire is sent to a new bank account

Threat actors claims they didn't receive the distribution, so a second wire is sent. Trustee attempts to reclaim first wire, FBI is involved. First wire is recovered, bank enforces 90-day waiting period before deciding the status of the second wire.

WHY REACTION TIME IS CRUCIAL

Timeline in the event of a claim

01

Notify your broker and cyber carrier

Typically, cyber carriers offer a 24/7 monitored hotline for insureds to call and initiate an incident response playbook

02

Engage Legal Counsel

This allows your to protect attorney-client privilege as your work through a cyber incident. Carriers have recommended firms that specialize in this area.

03

Engage a forensic expert

Providers are recommended by the carrier, and hired via legal counsel. They can help investigate, mitigate, identify impact, and remediate losses.

If there are lost funds, notify the FBI, law enforcement and banking institutions within 72 hours for best chance of recovering funds.

BEST PRACTICES

You are the first line of defense. Implementation and use will impact your cyber security, and underwriting profile positively.

VERIFY REQUESTS

Always confirm distribution requests & wire instructions via a secondary channel. Double & triple check instructions, especially if labeled as urgent

SECURE COMMUNICATION

Use secure, encrypted email or platforms for sending sensitive information

MONITOR REGULARLY

Frequently monitor accounts and transactions for any unusual activity

IMPLEMENT PROTOCOLS

Implement strong authentication methods, incl. multi -factor authentication, password protocols, using a verified cloud provider

UPDATE SECURITY MEASURES

Regularly update and patch your cybersecurity systems to protect against new vulnerabilities

INCIDENT RESPONSE PLAN

Have a robust incident response plan in place. This should include immediate step to take if there is a suspected breach or cyber event

SOME GOOD NEWS
MICROSOFT DEFENDER

There are accessible tools that can protect you and lessen the chance of a cyber incident.
Microsoft Defender can provide the following

ADDS A VPN AND DARK WEB SCANNER

SIMULATED PHISHING ATTACKS, POST AND RESPONSE, & AUTOMATION -BREACH INVESTIGATIONS, HUNTING

PROVIDES INVESTIGATION AND REMEDIATION CAPABILITIES TO HELP SECURITY TEAMS IDENTIFY, PRIORITIZE AND RESPOND TO THREATS

SAFE LINKS FEATURE PROTECTS USERS FROM MALICIOUS URLS IN A MESSAGE OR OFFICE DOCUMENT

PROTECTION FOR SHAREPOINT, ONEDRIVE, AND MICROSOFT TEAMS

ANTI -PISHING MONITORING ON INCOMING MESSAGES

CYBER LIABILITY INSURANCE 101

Cyber liability insurance helps cover costs associated with data breaches and cyberattacks on your business. Those costs can include such things as lost income due to a cyber event, costs associated with notifying customers affected by a breach, costs for recovering compromised data, costs for repairing damaged computer systems. More importantly it’s a service.

- Forensic investigations
- Litigation expenses
- Regulatory defense expenses/fines
- Crisis management expenses
- Business interruption
- System testing
- Cyber extortion
- Cyber crime - social engineering / fraudulent transfer

2025 CYBER MARKET TRUSTEE V INSTITUTION

The insurance market has been fairly stable from a pricing perspective.

- There are limited carriers willing to provide coverage for third party funds
- For large organizations, a combination of crime and cyber insurance is recommended for comprehensive coverage
- To build appropriate limits for e -crime, we build layers, called a tower
- MFA is a baseline requirement for most underwriters

UNDERWRITER EMPHASIS

01

THIRD PARTY RISK MANAGEMENT

Organizations must ensure vendors adhere to rigorous cybersecurity standards

02

MULTI FACTOR AUTHENTICATION & ZERO TRUST ARCHITECTURE

These security measures are increasingly being mandated for policy approval.

03

BEST PRACTICES AND RESPONSE PLANNING

Demonstrating comprehensive incident response plans are receiving more favorable policy terms.

LESSONS LEARNED

- Trustees do not have custody, but they do have care and control of third -party (customer/beneficiary) funds
- Fine line between E&O, Wire Transfer Fraud (crime) and cyber liability/social engineering (crime and cyber policy)
- Different policies have varying conditions
  - Required call back verification
  - Litigation/Subrogation expense
  - Exclusionary language
- Financial institutions liability (how and when decisions are made)
- Who else may have liability (vendors (back office/IT professional/ETC)

CONCLUSION AND KEY TAKEAWAYS

Get training - Training widely available through vendors like KnowB4 & Microsoft Defender

Get protected - Implementing best practices and basic software will impact the frequency and severity of losses

Get updates - stay up to date regarding latest trends, be proactive in cyber security. Human error is the leading cause of cyber events

Contact Us

Hannah DeLucca
Vice President, Precision Brokers LLC
hdelucca@precision-ins.com | 201.306.3414

Judy Pearson
President + CEO, Precision Brokers LLC
jpearson@precision-ins.com | 303.917.7766