Thank you to our sponsors for making CSMB events possible.
• **Convening** partners who recognize strength in the security collective

• **Educating** individuals and organizations on cybersecurity best practices

• **Amplifying** collective efforts to increase cybersecurity awareness
Thank you to our national sponsors.

*Our sponsors help us reach*

- Over 10K webinar attendees
- Over 5K workshop attendees
- Over 15K subscribers

2021 Sponsorships Available

**Signature Sponsor**  
2 slots available

**Contributing Sponsor**  
3 slots available

**Affiliate Sponsor**  
4 spots available

**Webinar Sponsor**  
Unlimited availability
Why we are talking about Cyber Risk and Cyber Insurance today

- Working in a remote world
- Threats are increasing
- Landscape is changing
- Resiliency
- Insurance is complex
Our Speakers

Matt Honea

Senior Director of Cybersecurity at Guidewire who has worked extensively in the areas of threat intelligence, network defense, system forensics and discovery, enterprise security auditing, malware analysis and physical security.

Matt was previously responsible for research and development on the Guidewire Cyence Risk Analytics platform, a risk modeling tool used widely in the cyber insurance industry. Matt is an industry speaker, author on cyber risk, and recipient of the 2019 Silicon Valley Business Journal 40 under 40 honor.
CEO at Transmosis, which is a nationally recognized cyber security workforce developer founded in Silicon Valley that enables American workers to develop new careers in the rapidly growing information security industry (www.transmosis.com).

Transmosis’s proprietary virtual cybersecurity security analyst training model serves as the foundation of CyberOPS, a military grade cyber security platform with fully integrated cyber liability insurance designed to protect small businesses from cyber attack (www.transmosis.com/cyberops).
Our Speakers

Dr. Olga Livingston

Senior Economist leading cyber economics analysis at the Cybersecurity and Infrastructure Security Agency (CISA). Olga has a background in Econometrics with extensive experience in applied economic modeling and risk analysis.

In collaboration with interdisciplinary teams of cyber security engineers and information security specialists, Dr. Livingston leads analysis on cyber incident costs and losses, effectiveness and economic justifiability of potential mitigations, cyber insurance, as well as the overall benefits of cyber security investments in reducing cyber risk.
You’re a small business

The CEO says you have 10k to spend on security
CYBERSECURITY VS. CYBER RISK

**Cybersecurity**

- Securing an organizations’ resources and people
- Programmatic
- Primarily technical factors and procedures
- Can be audited against frameworks

**Cyber Risk**

- Wholistic posture of an organization
- Impact analysis to include dependencies
- Both technical and non-technical factors
- Modeled behavior that incorporates human elements
AGGREGATED ATTACK DATA

**Top Sectors**
- **Education**
- **Business Services**
- **Hospitality**

**Easiest Targets**
- **Deepest Pockets**

**Top Vectors**
- **Ransomware**
- **Business Email Compromise**

**Ease of Deployment**
- **Reuse**

**High rate of payment**
- **High leverage points**
- **Weaker security mindset and controls/Double Whammy**

**Direct payments**
- **Ease of selling access**
- **Crypto appreciation**

*2020 Guidewire Data, < 1B USD, USA*  
National Cyber Security Alliance

Cyber Risk:
The Time Is Now To Understand Insurance and Risk

chase@transmosis.com | www.transmosis.com/cyberops
Small Businesses Think They’re Protected, They’re Not

› Most small businesses believe that Antivirus and Firewall are enough to protect them
  › **They’re Wrong**

› Small Businesses are the #1 target for cyber criminals today with more than half of all attacks last year, resulting in the majority closing within six months.

› The average ransomware payout is now $177,000, WFH making matters worse.

› 83% of Small Businesses don’t carry cyber liability insurance and many think their existing GL policy covers cyber.

› Reputational damage from a breach can be devastating (**first party**).

› Small businesses are liable to their partners (**third party**).

› Large companies working with small businesses increasingly require higher cybersecurity standards and cyber liability insurance.
First Party Liability

Damage from attacks on the small business’s own network or system or vendor’s system. First-party damages can include the costs associated with notifying affected customers and employees of a data breach.

- Data breach/theft, ransomware, extortion.

Results in:

- Reputational damage.
- Data recovery expense, pr, legal, forensics.
- Business downtime (loss of revenue).
Third Party Liability

Damage from connections to third parties (partners, customers, vendors). Third-party damages include the legal aspects of a data breach, particularly in the legal fees and costs of settlements, civil awards, or judgements resulting from a lawsuit.

Results in:

- Lawsuits.
- Cancelled contracts, larger companies drop you.
- Regulatory fines
  - New laws in states like NY and CA impose harsh fines for consumer data breaches even if your company doesn't reside there.
Research

Finding the right Cyber Insurance

- First off, research is time consuming and difficult.
- Not clear what policies will cover, fine print, carve-outs (social engineering), approved technology, sublimits, etc.
- Insurance brokers not great at selling cyber insurance.
- Requires ongoing diligence to ensure correct policy is in place.
- Not maintaining IT controls/updates could jeopardize claim payments.
Cyber Policies

› **What SMBs should look for in Cyber policies**

› Integrated technology and cyber liability policy where insurer stands by the provider.

› **First Party coverage:**

› Business interruption expenses, cyber extortion reimbursement, legal expenses, forensic expenses, compliance expenses.

› **Third Party coverage:**

› Liability costs centered on network security, privacy liability or electronic media – such as trade libel, plagiarism or copyright / trademark infringement.

› Additional Endorsements: policy add-ons like invoice manipulation, betterment (system replacement and upgrade), system failure (business interruption due to human error), additional insured, etc.
Cyber Insurance Trends

- Fastest growing category of commercial insurance.
- The global cyber insurance market is projected to grow by 21% in 2021, reaching $9.5bn in value.
- Making its way from enterprise to SMB.
- However, increase in attacks making insurers and reinsurers nervous.
  - Rates going up.
  - Not enough long-term data on claims.
- Increasing trend towards integration of cyber technology and insurance.
  - Reduces risk for both parties.
National Cyber Security Alliance

Cyber Risk:

The Time Is Now To Understand Insurance and Risk

chase@transmosis.com | www.transmosis.com/cyberops
CYBER RISK AND INSURANCE

NCSA WEBINAR
CYBER RISK: THE TIME IS NOW TO UNDERSTAND INSURANCE AND RISK
MARCH 2, 2021

DR. OLGA LIVINGSTON
Decision Context

Business Objectives: Profit & Growth

Attracting New Customers
Retaining Existing Customers
Complying with Regulations
Cybersecurity
Attracting Talent
Ensuring Physical Security
Financing

Cyber Risk Management Strategies

Avoid
Reduce
Transfer
Accept

Controls and Mitigations
NIST Cybersecurity Framework
NIST 800-53
Outsourcing
Contractual Agreements
Cyber Insurance
Risk Sharing and Pooing
Cybersecurity is a business support function.

For small and medium-sized businesses (SMBs), cybersecurity ranks 3rd or 4th among business priorities.

Cyber risk ranks 5th among other risks.

Risk transfer is one of the four cyber risk management strategies.

Cyber insurance is a risk transfer tool – it transfers risk for select cyber incidents by offsetting some of the following costs: investigating and containing an incident, cleanup and recovery, victim notification, credit monitoring and ID protection, legal fees and settlement, etc.
BIA contributes to understanding and quantifying the loss of functionality for various system types and the supported mission function or revenue stream.
Resources for BIA

- CMU-SEI Business Impact Analysis Report – A loss magnitude estimation in support of BIA.
- Cyber incident cost for SMBs:
  - NetDiligence Cyber Claims Study 2020 Report – Cost by loss category, revenue size, industry, and incident type.
  - Hiscox Cyber Readiness Report – Total cyber incident cost and other useful facts. Prior years reported incident cost by SMB size.
- IRIS 20/20 – Cyber incident frequency and cost by industry and business size.
- Verizon 2020 DBIR – Prevalent incident types by industry.
Basics to Protect Yourself

Things to Do First

- Back up Data
- Multi-Factor Authentication
- Patch & Update Management

Getting Started

- Cyber Essentials | CISA
- Cyber Essentials Toolkits | CISA
- Ransomware Guidance | CISA
Many companies forego policies due to what they perceive as high costs, confusion about coverage, and uncertainty about suffering a cyber-attack.

Source: CISA Cyber Insurance Market Assessment Report
Understand the coverage and exclusions.

1. Do not assume cyber is included under the traditional coverage.

2. Clarify covered incident types, cost and loss categories, limits and sublimits, and exclusions.

3. Clarify what is included in the service offering (e.g., bundled post-breach services, risk mitigation assistance, or only partial reimbursement of incident cost).

4. Understand specific requirements (e.g., a need to have an incident response plan in place, which crisis management company to contact, and the preferred digital forensics and incident response provider).
Panel Discussion
Q + A
Thank you for joining us!

Twitter: @staysafeonline
Website: staysafeonline.org
Email: info@staysafeonline.org

Cyber Secure My Business
Staysafeonline.org/cybersecure-business