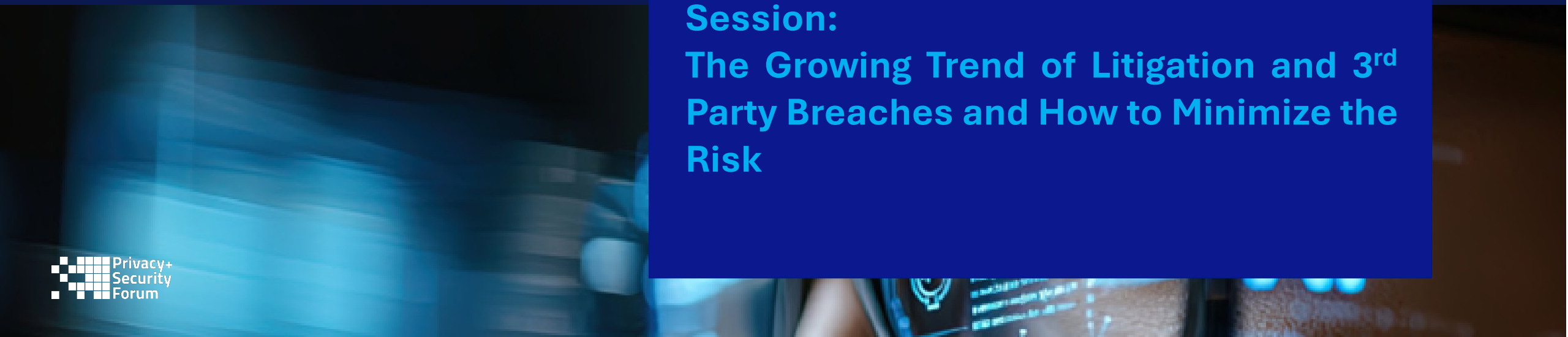
Privacy + Security Forum

Session:
The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk



Speakers: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Melanie Witte
Manager – eRisk Claims
Crum & Forster

John Lancaster
Senior Director, Response
Surefire IR

Kamran Salour
Co-Chair, National Cybersecurity and Data Privacy
Lewis Brisbois

Jenn Doe
Vice Chair, National Cybersecurity and Data Privacy
Lewis Brisbois

Privacy+ Security Forum

CF EST. 1822 A FAIRFAX COMPANY

SUREFIRE CYBER

LEWIS BRISBOIS

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Session Agenda

- Cyber Incidents Skyrocket
- Simple Measures for Network Security
- Data Breach Class Actions Explode
- Third-Party Breaches Present Increasing Risk & How to Minimize that Risk
- Audience Q&A

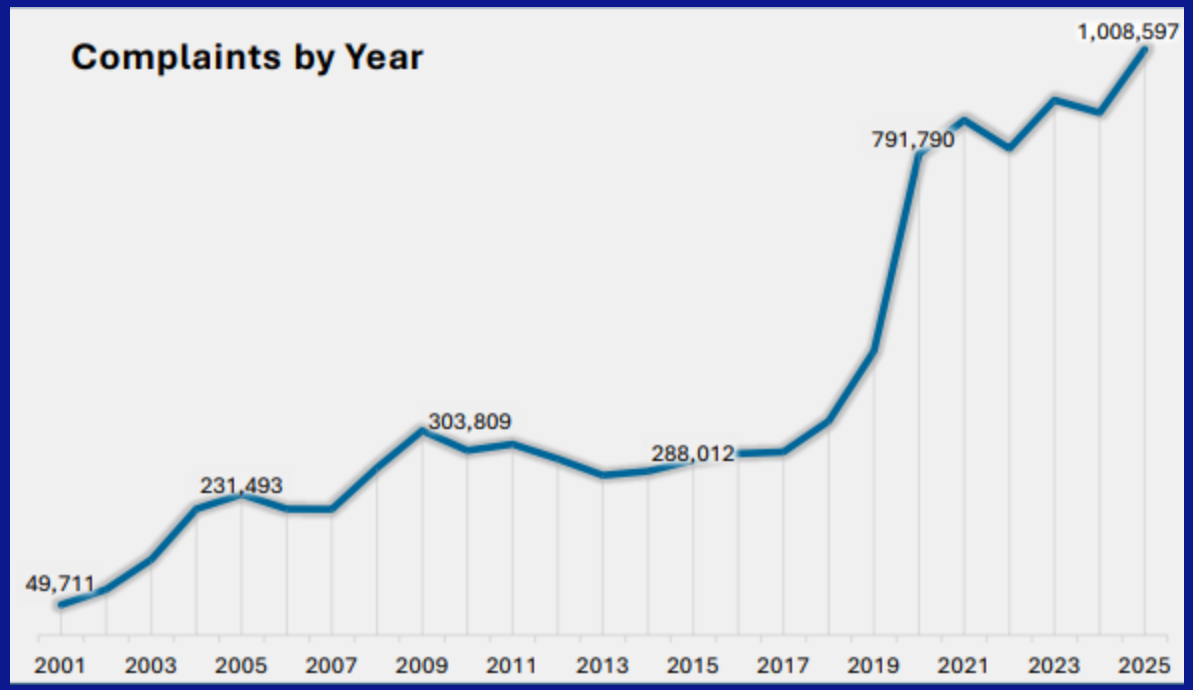
Privacy+ Security Forum

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Cyber Incidents Skyrocket

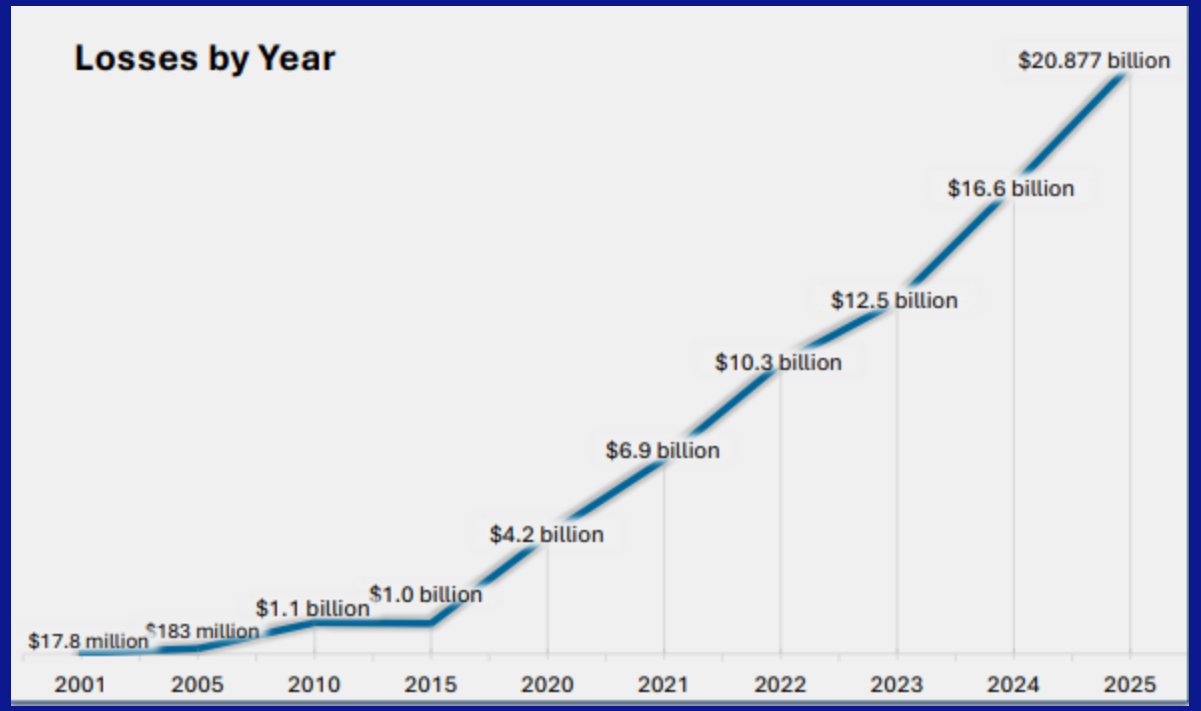
Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Cyber Incidents Reported to FBI Per Year



Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Cyber Incident Related Losses Reported to FBI



Privacy+ Security Forum

CF EST. 1822 A FAIRFAX COMPANY

SUREFIRE CYBER

LEWIS BRISBOIS

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

- Most frequently targeted sectors include healthcare and public health (clinics, hospitals, etc.), financial services (banks, credit unions, etc.), law firms, government entities (towns, cities, electric companies, electric co-operatives, etc.), and contracting services.
- Most ransomware attacks involve the exfiltration of large amounts of data.
- Most victims have sensitive data (i.e. SSNs, DL numbers, health records, medical insurance information, passports, etc.) stored in their network environments.
- Exfiltration of these types of sensitive data generally leads to individual and regulatory notification obligations, which lead to……

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Simple Measures for Network Security

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Simple Security Measures

- Network Segmentation – separate assets that may store critical data (database servers, file servers, other critical infrastructure servers) into their own VLANs and control access to those assets
- Enforce least-privilege access – users and services should only be able to reach network resources they need. Use ACLs, firewall rules, and zero-trust principles to deny access to resources
- Use strong authentication everywhere possible – enable MFA on VPN, web admin consoles, and RMM tools

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Simple Security Measures Cont.

- Deploy monitoring and logging – EDR, log aggregation/analytics (SIEM) to alert on things like lateral movement and program execution
- Disable unnecessary ports and services – reduce surface risk on assets where/when possible
- Have an incident response plan – know what to do, who to call, what to isolate, and how to contain in the event an incident occurs
- These measures should be part of an ongoing security audit (NOT A ONE TIME TASK!)

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Data Breach Class Actions Explode

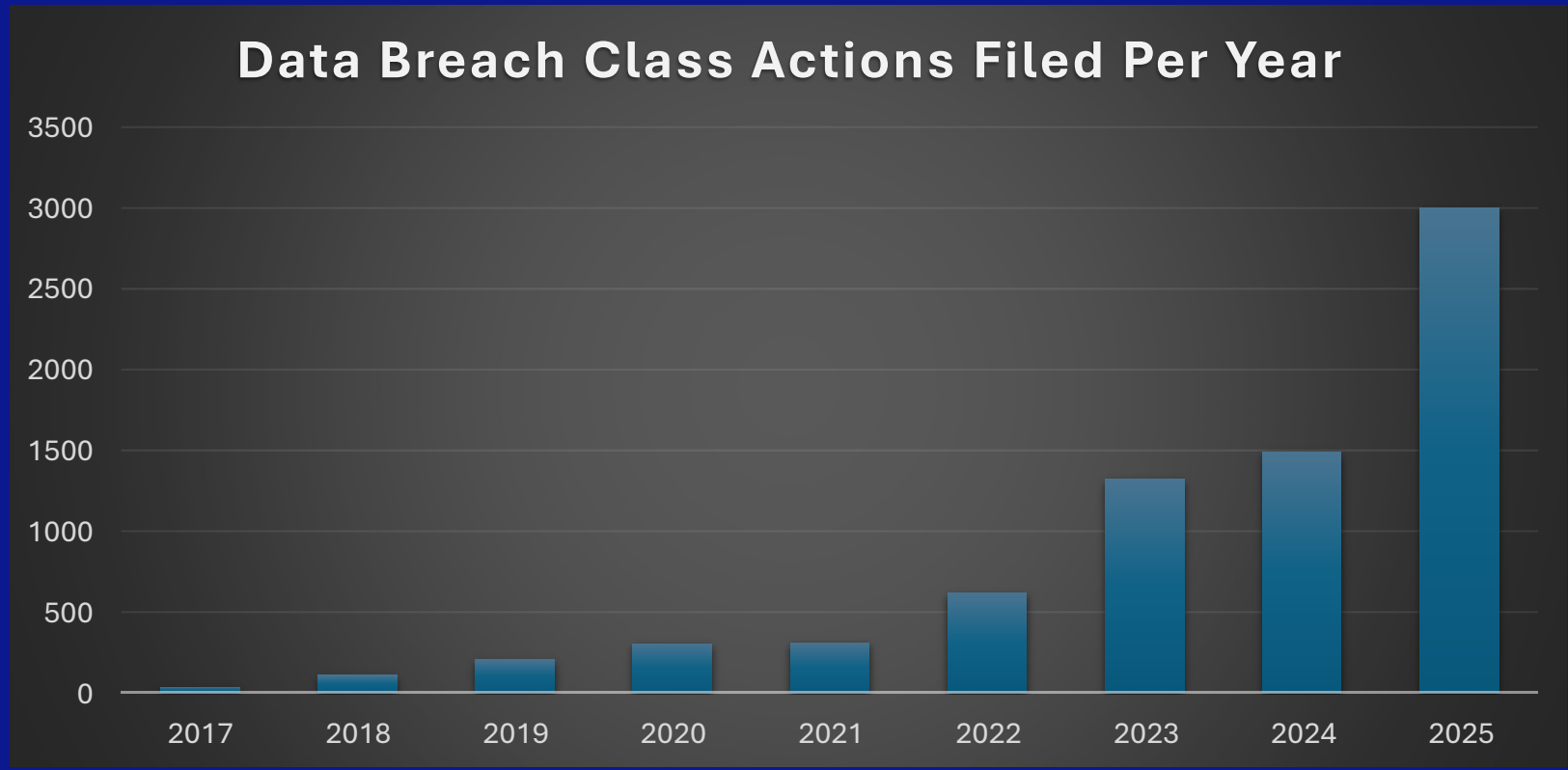
Privacy+ Security Forum

CF EST. 1822 A FAIRFAX COMPANY

SUREFIRE CYBER

LEWIS BRISBOIS

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk



Privacy+ Security Forum

CF EST. 1822 A FAIRFAX COMPANY

SUREFIRE CYBER

LEWIS BRISBOIS

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

- A lot of factors dictate the size of a class action settlement, which are wide ranging.
- Some recent data breach class action settlement amounts:
  - Endue Software Settlement (17th Jud. Cir. Ct., Florida): $870,000 settlement across 28,968 individuals ($30/person)
  - AGC America Settlement (N.D. GA): $597,000 settlement across 20,592 individuals ($29/person)
  - New River Electrical Settlement (Cnty. Ct., Ohio): $425,000 settlement across 9,845 individuals ($43/person)

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

- Recent class settlements continued:
  - Phil Smith Auto Group (S.D. Fla.): $374,633 settlement across 13,145 individuals ($29/person)
  - Chattanooga Heart Institute (E.D. Tenn.): $3.75 million settlement across 460,000 individuals ($8/person)
  - Anne Arundel Dermatology (D., Maryland): $2,400,000 settlement across 1,905,388 individuals ($1.25/person)
  - Alabama Ophthalmology Associates (Jefferson Cnty. Cir. Ct., Alabama): $850,000 settlement across 153,575 individuals ($5.53/person)

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

- Pre-incident measures that can be taken to lessen risk to litigation:
  - Good network security hygiene
  - Encrypt at rest all sensitive data
  - Limit sensitive data residing on network environment

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

- Post-incident measures that can be taken to lessen risk to litigation:
  - Retain experienced breach counsel
  - Notify only those individuals whose information was impacted
    - Blanket notice should be exception – not rule
    - Use forensic investigation and threat actor communications to pinpoint data impact
    - Analyze results to build accurate and limited notice list

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Third-Party Breaches Present Increasing Risk & How to Minimize that Risk

Privacy+ Security Forum

CF EST. 1822 A FAIRFAX COMPANY

SUREFIRE CYBER

LEWIS BRISBOIS

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

3rd Party Breaches.....

Privacy+ Security Forum

CF EST. 1822 A FAIRFAX COMPANY

SUREFIRE CYBER

LEWIS BRISBOIS

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

- Businesses are increasingly reliant on outside vendors to host data
- Most companies provide sensitive information to cloud companies including Electronic Medical Records (EMR), human resource data, background check information, medical billing information, collections information, data transfer tools, etc.
- **98% of organizations use at least one third-party vendor that has experienced a breach in the past 2 years** (2024 SEC Cybersecurity Rules Update citing a report from SecurityScorecard and the Cyentia Institute)
- Threat actors know this and can strategically attack one victim and gain access to data from many entities

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Recent large scale 3rd party data breaches include:

- **TeamViewer (2016):** Impacted millions of TeamViewer accounts and permitted unauthorized access to many systems
- **SolarWinds Supply Chain (2020):** Threat Actors compromised Orion software platform that impacted 18,000 customers including major government agencies and Fortune 500 companies
- **Microsoft Exchange Server (2021):** Software vulnerability that impacted over 250,000 servers
- **Accellion File Transfer (2021):** Exploitation of outdated File Transfer Appliance software to exfiltrate sensitive data involving major corporations, government agencies and universities

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Recent large scale 3rd party data breaches include:

- **Kaseya MSP Platform (2021):** Threat Actors used the VSA software to deploy malware to Kaseya's downstream customers (estimated 800-1,500 companies globally)
- **Okta (2022):** Involved a compromise of Sykes (Okta's customer support vendor) that impacted approximately 2.5% of Okta's customer base
- **MOVEit (2023):** Ransomware that impacted over 2,000 organizations and approximately 62,000,000 individuals.
- **PowerSchool (2024):** US based Threat Actor accessed PowerSchool's cloud-based network to exfiltrate data impacting approximately 62 million students and 9.5 million teachers

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Consequences of 3rd Party Breaches

- Companies spend significant time and resources securing their own environments, but often pay little attention to exposure from vendors and cloud providers
- Ignoring these risks can lead to impactful financial consequences as well as reputational harm
- Ignoring the risks of a 3rd party breach can lead to not only being named in a class action lawsuit, but also open yourself up to a regulatory investigation for having entrusted your sensitive data to a breached company

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

How to Limit Risk

- In your Incident Response Plan, complete a data flow diagram. Identify all vendors that store your company's PII/PHI
- Identify all fourth-party vendors who may have access to this same information
- Conduct periodic audits
- Ask the tough questions…

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Questions to Ask 3rd Party Vendors that Store Sensitive Data

- Have you had any data breaches or cyber incidents in the past 2 years?
- Where do you store our data?
- How do you protect the data?
  - Any access control measures?
  - Encryption at rest?
  - Patch management?
  - EDR/XDR?
  - What physical security measures are in place?
  - Do you conduct regular security testing? Specify.
  - Are you compliant with relevant regulations and standards (i.e. HIPAA, GDPR, etc.)?

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Questions to Ask 3rd Party Vendors that Store Sensitive Data

- Do you have ongoing employee security training? How often?
- Do you have an Incident Response Plan? If so, please describe.
- Do you send our data to additional vendors/contractors?
  - If so, how do they store our data?
  - What security is in place?
  - Do they have an incident response plan?
  - Are they compliant with applicable regulatory standards?
  - Are you aware of any breaches on their side over the past 5 years?

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Contractual Measures with Third Parties to Limit Risk

- Ensure that the third-party vendor has cybersecurity insurance....and CONFIRM SUFFICIENT LIMITS!
- Include notice obligations with specific notice timeframes for any cyber incident
- Define specifically what constitutes a cyber incident or “breach” triggering notice to you
- Include language that confirms the company’s security measures purportedly in place

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Contractual Measures with Third Parties to Limit Risk

- Include language that requires the vendor to either return or destroy the data within a reasonable use timeframe
- Mandate that the vendor is liable for all breach related costs
- More importantly, mandate that the vendor is required to satisfy all incident-related data breach notification obligations to both individuals and regulators.

Session: The Growing Trend of Litigation and 3rd Party Breaches and How to Minimize the Risk

Q&A

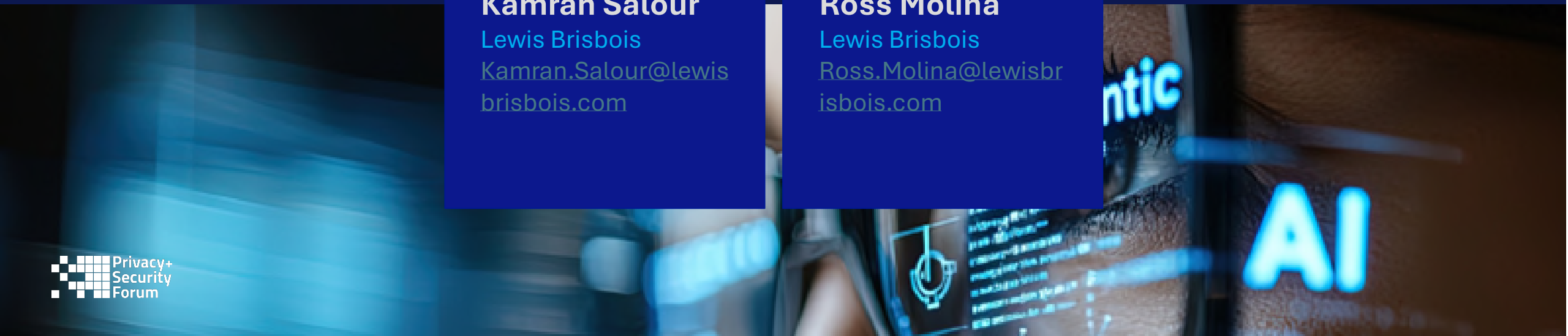
Stay in touch: Continue the conversation with us

Melanie Witte
Crum & Forster
Melanie.Witte@cfins.com

John Lancaster
Surefire IR
jlancaster@surefirecyber.com

Kamran Salour
Lewis Brisbois
Kamran.Salour@lewisbrisbois.com

Ross Molina
Lewis Brisbois
Ross.Molina@lewisbrisbois.com



Privacy+ Security Forum