

The Cyber Security Symposium Series

Prepare to Win: Building the framework for a comprehensive cyber security plan

April 20, 2021

Presented by



Today's Webinar: Housekeeping Items

- Today's webinar is being recorded.
- Attendees will be in listen mode with microphones automatically muted upon entry.
- For optimized viewing, we suggest that you change the screen view by hovering over the top right of speaker panels and choose Side by Side View.
- Questions are encouraged. Please enter them into the Chat feature.

How to prepare for the next cyber security threat.

- Welcome
- About Synovus, Carr Riggs & Ingram and Sylint
- Introductions
- Presentation
- Q&A
- Closing Remarks

Host and Moderator



Kevin Gillen

Symposium Host

Market Executive SW FLA,
Synovus



Mary Harrington

Symposium Moderator

Treasury & Payment Solutions,
Synovus

Presenters



Daniel Krug

Business Advisor,
Northwest Region
Cybersecurity
Program Manager

FloridaMakes



Alfred Saikali

Chair, Privacy & Data
Security Practice

**Shook, Hardy &
Bacon, LLP**



Andy Sekela

Special Agent,
Private Sector
Coordinator

FBI



Marc Schein

CIC, CLCS
National Co-Chair,
Cyber Center of
Excellence

**Marsh & McLennan
Agency**



Serge Jorgensen

Founding Partner
and Chief Technology
Officer,

Sylint Group



Byron Shinn

CPA and Engagement
Partner

**Carr Riggs & Ingram,
CPA, LLC**

74% of companies were targets of payments fraud in 2020, demonstrating the crucial need for cybersecurity protocols, employee training and strict control governance.

76% of organizations experienced Business Email Compromise (BEC)

50% of BEC scams targeted ACH debits & credits and Wires targeted at **43%**

61% of BEC attempts are targeted at Accounts Payable teams

66% of organizations experienced check fraud

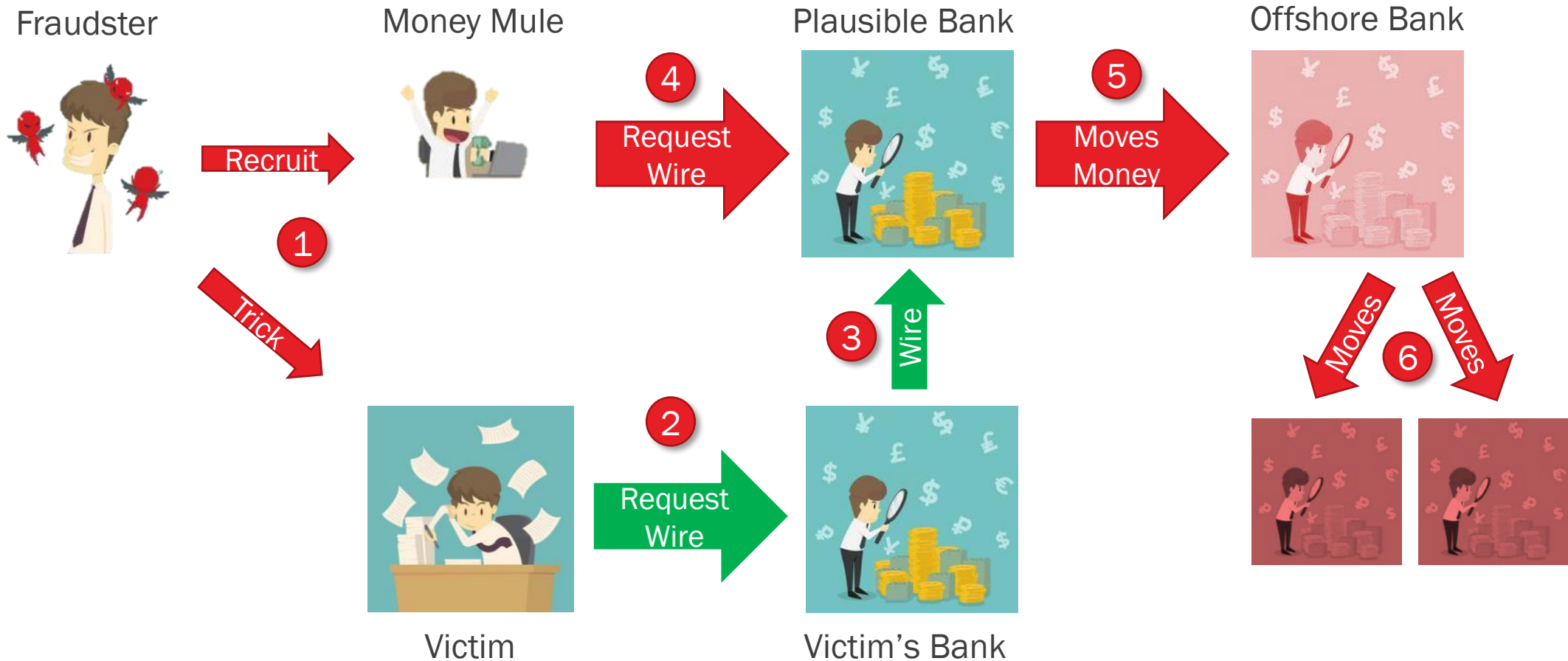
34% of payments fraud targeted ACH debits and **19%** for ACH credits representing continued increases for both payment types

80% of companies are leveraging education and training on the BEC threat and how to identify spear phishing attempts

Topics

- FBI: scope, scale, difficulties & success
- Insurance: cautions, and some solutions
- Finance & Legal: laws, audits & requirements
- Trade Assoc: more solutions
- Symposium wrap & key components

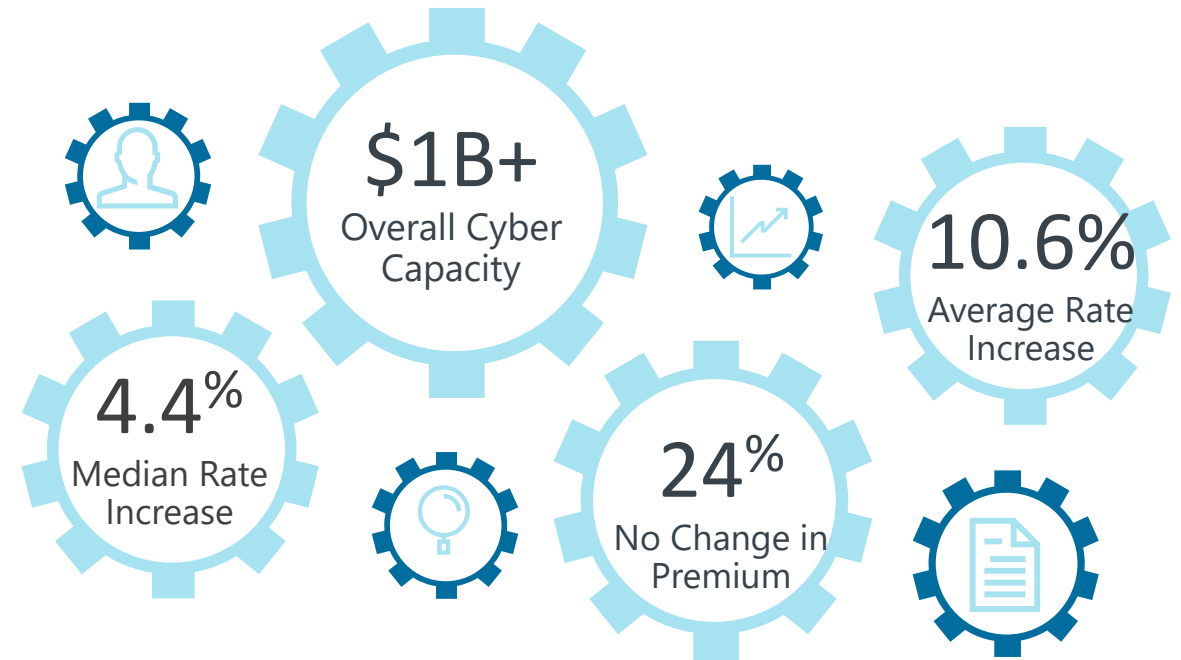
BEC Workflow & Recovery Challenges





US Cyber – Q3 2020 Market Update Highlights

- In the third quarter of 2020, total program cyber rates increased by an average of 10.6%. The median renewal was up 4.4%.
- In the third quarter of 2020, primary cyber rates increased by an average of 10.7%. The primary median renewal was up 4.8%.
- 24% of clients renewed with no change in premium and 14% of clients achieved a decrease.
- Primary cyber increases have caught up with excess rate increases. This analysis ends four quarters where excess pricing increased more than primary pricing.
- September 2020 was the most active month on record for ransomware claims, as verified by leading cyber insurers. Ransom payments and resulting business interruption claims are the main factors contributing to these increases.



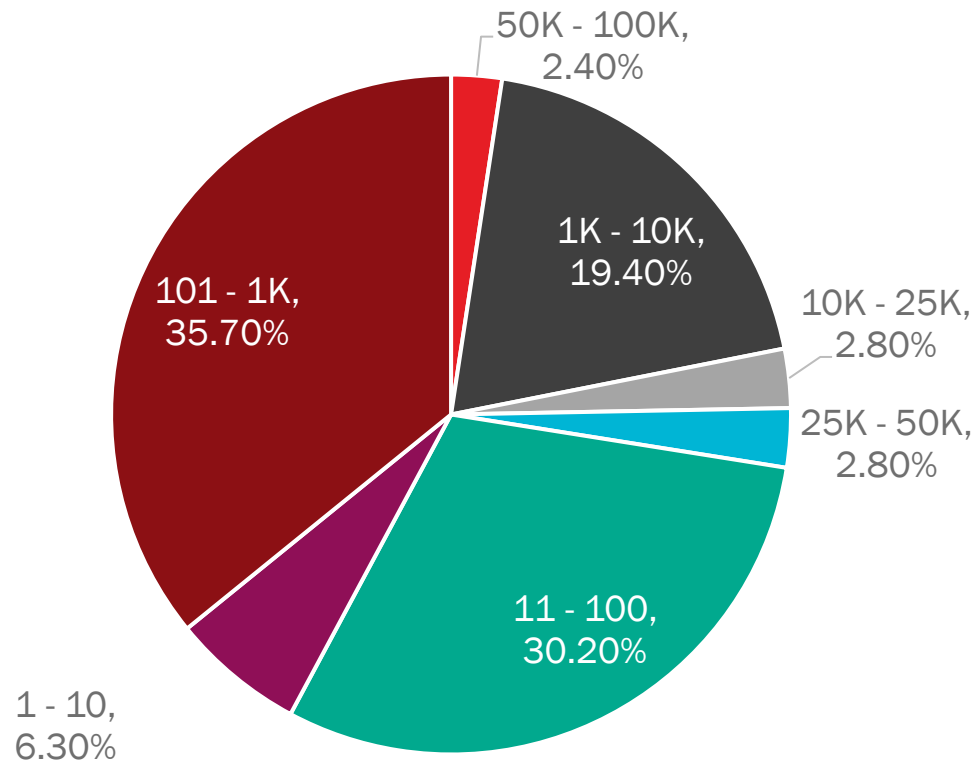
Cyber ranked 5th* in areas where risk is expected to increase

- In 2021, cybercrime damages might reach \$6 trillion

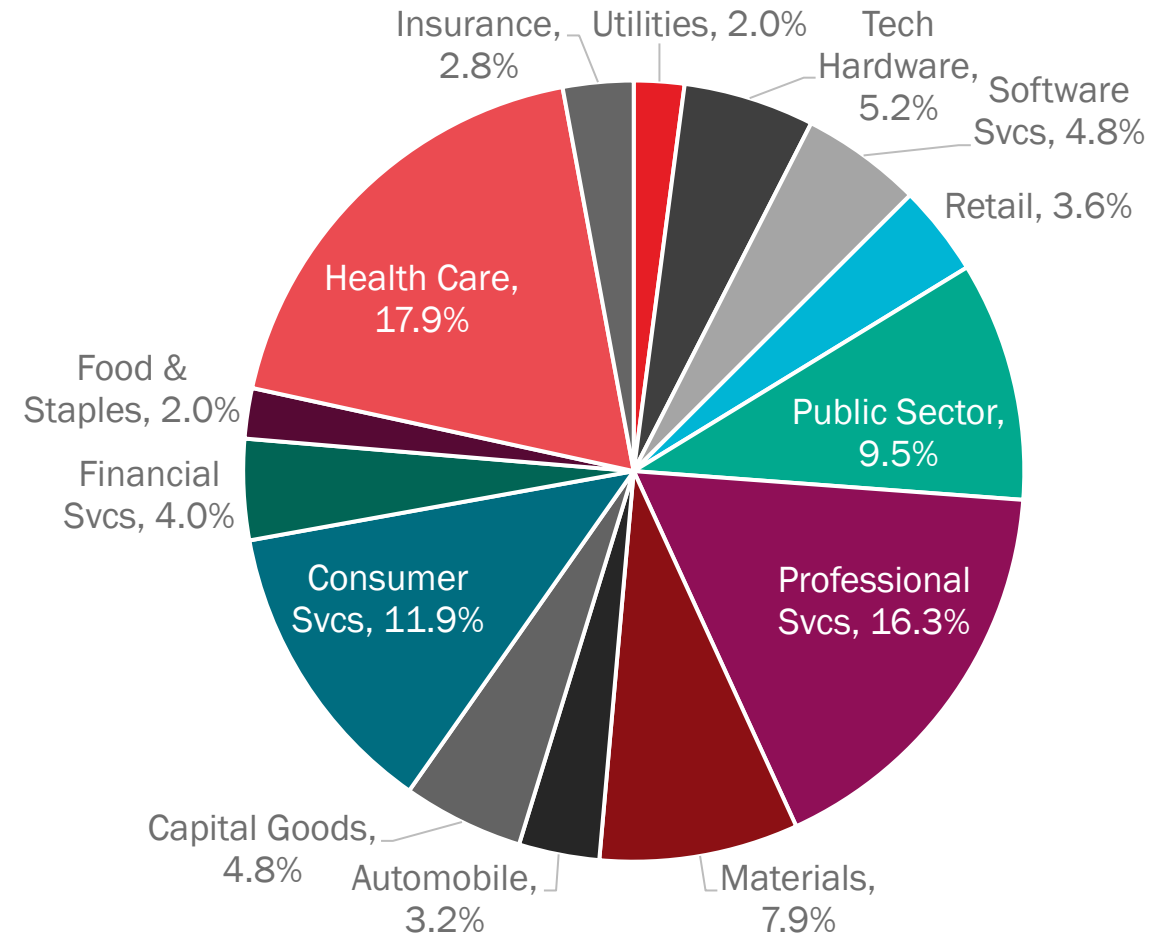
Equivalent to the GDP of the world's third largest economy.

BEC Distribution

Company Size (Employee Count)



Industry



State of the Cyber Insurance Market & Forecast 2021

1. Q2 Forecast: 30-50%+ Cyber insurance rate increases (*assuming adequate controls and static exposure*)
2. Some carriers non-renewing entire cyber insurance portfolios
3. Potential continued cyber carrier exits from market & reduced capacity
4. Ransomware supplemental applications (RSAs) required
 - In many cases, a 'mainform' application is recommended for full marketing efforts and u/w detail (remove warranty Q's)
 - We recommend insureds elaborate on responses (i.e. incl. timelines for security control implementations)
5. Carrier A implementing 50/50 coinsurance, halved ransomware event coverage sublimits, moved to non-admitted paper on top of continued rate increases
6. Carrier B implementing 50% max sublimit for contingent business interruption (CBI) coverage
7. Some leading markets adding "SolarWinds impact" exclusions; "End of life software" exclusions
8. Minimum security controls that are strongly recommended:
 - MFA, Disable RDP for all external access, Encryption & Segmentation, Tested Backups, Endpoint Detection and Response (EDR), Employee Awareness Training, Firewalls, etc.
 - Need to be in place if at all possible. Risk that do not have these controls in place are seeing even higher increases in pricing / deductibles, reduction in coverage/limits or non-renewal.

Embedding Cyber Risk in EH&B Client Conversations

62% of executives say the greatest threat to their organization's cybersecurity is employees' failure to comply with data security rules, not hackers or vendors

(Mercer's 2020 Global Talent Trends Study).

Why HR's Role is Important:

- Pervasive use of technology and devices in employees' work
- HR is instrumental in building cybersecurity culture, employee training and awareness programs
- HR's coordination is essential when a cyber incident occurs
- More active regulatory environment

Cyber covers more than just IT:

- Coverage Includes 1) Incident Response 2) Liability & Regulatory 3) Business Interruption/Extortion
- Proactive services included in policy – employee training & incident response preparation
- To be a trusted advisor, we owe it to be proactive in connecting cyber risk with HR

Insurance & Brokers as Part of the Solution

- Rapid hardening of the cyber insurance market
- Increased underwriting scrutiny
- Insureds looking to increase their cyber maturity
- Companies are offering Proactive (per-loss) solutions
- Coverage may be dictated by cyber-security posture

Florida Cyber Security Update

- Recommendations from the Governor's Florida Cybersecurity Task Force chaired by the Lt. Governor
- Senate Bill 1900 sponsored by Sen. Jim Boyd of Bradenton
- New Law will **require** protection mandated in order to protect Florida data bases and businesses relying on the information.
- The 37 different agencies will be required to build the safeguards into their operations and protect independent verification of compliance to the NIST standards.
- This will likely become the standard for all counties and cities throughout Florida

Details of the Cybersecurity Law

- Require
 - annual *independent* **Cybersecurity Risk Assessment**
 - **Action Plan** to cure areas noted in the assessment
- Develop an **Incident Response Plan**
- Develop a **Cybersecurity Recovery Plan**
- Organizational team **Practice Sessions** (e.g., Tabletop Exercises)
- Require **Qualified Employees** to be in key positions and maintain certifications
- Maintain plan to engage **outside help immediately** with a large scale incident

Preparation

- Homeowners and businesses know
 - what they are **supposed to do** and **where to go** in the event of a hurricane,
 - **what is covered** by Insurance, and
 - **who to call** if something happens.
- What would you do in the event of a cyber attack?
 - Who would you call first?
 - Insurance coverage, limits and areas not covered
 - Legal Team
 - Communications (requirements for disclosure and timing)



Other Considerations

- New Legislation Enhancements

- Contracts dealing with vendors will be exempt from the Florida Sunshine Law.
- Meetings with governance will be exempt from public records request and exempt from meeting in the sunshine.

- Regulatory Agencies Involved

- State Attorney General
- SEC, FTC, OCR ...

- Privacy and Data Security Laws & Requirements

Legal Issues to Consider

- How to engage a forensic firm to maximize privilege
- Ransomware - whether to pay the ransom
- Whether the incident is a notifiable event, who to notify, and when
- Engaging law enforcement
- Liability created by statements to employees and public
- Evaluating potential third-party liability and indemnification
- Cyber insurance coverage/exclusions

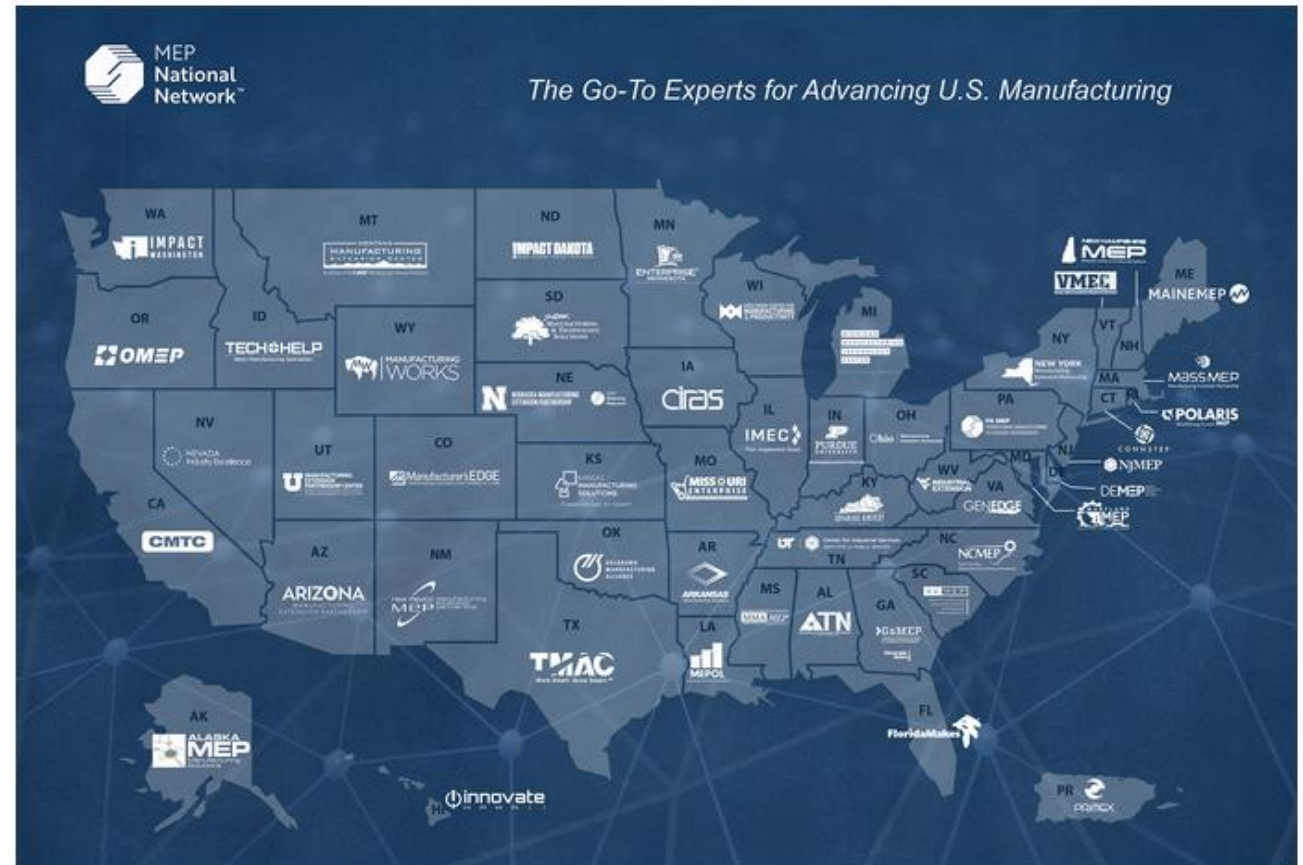
Now What?

- Basic Preparedness
 - Synovus resources
 - Marsh & McLennan and other insurance solutions
 - Frameworks, Standards & Integration with existing programs
- Specific Resources
 - Broker/Insurance Driven
 - Government Offered (CISA, Center for Internet Security, National Institute of Standards and Technology)
 - Trusted Partners (CPA, Counsel, Bankers...)
 - Trade Groups



FloridaMakes and NIST MEP

- NIST Manufacturing Extension Partnership
 - Public-private partnership
 - 51 Centers
 - Over 1400 trusted advisors
 - Provides US manufacturers with access to resources they need to succeed
- FloridaMakes
 - Florida MEP



Florida Defense Cybersecurity Training Program



The banner features a blue background with a globe on the left and various cybersecurity icons like padlocks and keys. The title "Florida Defense Cybersecurity Training Program" is centered in large white text with a drop shadow. Below the title are logos for DEO (Florida Department of Economic Opportunity), FloridaMakes, and OEA (Office of Economic Assistance).

Presented in partnership with:



Understanding Compliance

- NIST 800-171
- DFARS 252.204-7012
- NIST HB 162
- DoD Assessment Methodology
- Federal Contract Information
- Cybersecurity Maturity Model Certification Levels 1-5
- Cyber Attacks



Defense Federal Acquisition Regulations Supplement (DFARS) Clauses

- 252.204-7012 – Safeguarding CDI and Cyber Incident Reporting (2013)
 - Self- Attestation
 - 2017 Deadline
- NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (2016)
 - 110 Security Controls, 14 Security Requirement Families – MINIMUM Requirements
 - System Security Plan
 - Plan of Action with Milestones

...and more DFARS Clauses

- **252.204-7019** – Notice of NIST SP 800-171 Assessment Requirements (30 Nov 2020)
 - “Basic Assessment” – Contractor Self-assessment using DoD Assessment Methodology
 - Assessment score uploaded to Supplier Performance Risk System (SPRS)
 - Plan of Actions with Milestones & Date that all requirements are expected to be implemented
- **252.204-7020**
 - “Medium” or “High” Level Assessment
 - Performed by DoD personnel
- **252.204-7021** – Current CMMC Certification
 - Insert clause in all subcontracts
 - Subcontracts also required to be CMMC Certified





Key Components

COMPREHENSIVE CYBER SECURITY PLAN

Components of a Solution

Planning

- Threat Awareness
- Low Hanging Fruit
- Proper Tools



Preparation

- **Define** events, incidents, and breaches
- **Provide** escalation instructions
- **Identify**
 - internal stakeholders
 - external support and important contacts
- **Determine** how to engage, application of privilege and work product protection
- **Create** documentation process
- **Develop** communication & notification templates



Knowledge: Threat Awareness Briefings

- Insider Threat
- Economic Espionage
- Business Email Compromise
- White Collar Crime
- Internet & Investment Fraud
- COVID-19 Fraud Schemes
- Basic Cybersecurity Tools & Techniques
- Cybersecurity Trends (Parts 1 & 2)
- Foreign Influence
- Public Corruption
- Election Crimes
- Contract Corruption
- Counterintelligence



Help from Partners both Proactively & Responsively

- Insurance & Brokers
- Trade Groups
- Professionals (CPA, Legal, Cybersecurity, Bankers, Security Partners)
- Frameworks & Solutions (www.cisecurity.org, www.nist.gov/cyberframework)



Cyber Security Series - Panelist Contact Information

Enrique A. Fernandez	Director of Financial Crimes Unit	Synovus	enriquefernandez@synovus.com
Kevin Gillen	Market Executive	Synovus	Kevingillen@synovus.com
Mary Harrington	Technical Sales Consultant	Synovus	maryharrington@synovus.com
Serge Jorgensen	CTO	Sylint Group	sjorgensen@sylint.com
Daniel Krug	Business Advisor, NW Region Cybersecurity Program Manager	FloridaMakes	Daniel.krug@floridamakes.com
Larry Kunin	Partner	Morris Manning and Martin LLP	lhk@mmmlaw.com
Alfred Saikali	Chair, Privacy & Data Security Practice	Shook, Hardy & Bacon, LLP	asaikali@shb.com
Michelle Schauerman	Breach Response Services Manager-Cyber & Executive Risk	Beazley Group	michelle.schauerman@beazley.com
Andy Sekela	Special Agent, Private Sector Coordinator	Federal Bureau of Investigation	asekela@fbi.gov
Marc Schein, CIC, CLCS	National Co-Chair Cyber Center of Excellence	Marsh & McLennan Agency	Marc.Schein@marshmma.com
Byron Shinn	Partner	Carr Riggs & Ingram	bshinn@cricpa.com
Joseph W. Swanson	Attorney at Law	Carlton Fields	JSwanson@carltonfields.com
Robert Villanueva	EVP, Global Cyber Fraud Threats, E-Crimes Intelligence	Q6 Cyber	rv@q6cyber.com
Paul Vitchock	Supervisory Special Agent,	Federal Bureau of Investigation	pjvitchock@fbi.gov

Resources

Synovus

- Cyber Security Webinar Series - <https://www.synovus.com/business-webinar-series/>
- Safety and Security - <https://www.synovus.com/contact-us/safety-and-security/>
- Personal Resource Center - <https://www.synovus.com/personal/resource-center/#security>

FBI Internet Crime Complaint Center (IC3)

- <https://www.ic3.gov/default.aspx>

Federal Trade Commission

- <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

U.S. Small Business Administration (SBA)

- <https://www.sba.gov/managing-business/cybersecurity>

U.S. Department of Homeland Security – U.S. Computer Emergency Readiness Team (US-CERT)

- <https://www.us-cert.gov/ccubedvp/smb>

Thank you for attending

A brief survey will be sent to you from Events@Synovus.com.

Thank you in advance for your time and feedback.



Appendix





Kevin Gillen

Symposium Host

Market Executive SW FLA,
Synovus

Kevin has over 40 years' experience in the banking industry. He is Market Executive for Synovus Bank in the Florida Division comprised of 72 full service commercial branches. Kevin supports the commercial, business banking and retail sales, marketing and business development strategy and new hire on boarding for the commercial and business bankers in Florida.

He was previously Director of Supply Chain Strategy for Private Eyes Inc. and 4506 Transcripts; two companies, same ownership. Private Eyes is a Global Employment Background & Drug Screening Company. 4506 Transcripts.com is a large IRS bulk approved vendor for tax transcripts integrated with Fannie Mae, Ellie Mae.

Kevin was Executive Vice President, Retail Lending Director for TD Bank which included a \$36Bn residential mortgage and home equity portfolio. He was responsible for product development, pricing, secondary market sales, risk, US sales.

Prior to this role, Kevin was, EVP- Head of Retail Strategy and Solutions for TD Bank. He was responsible for US Retail Sales, Operations, Distribution, Risk, ATM and the Contact Centers. Total operating budget was \$1.6Bn with 14,000 employees.

Previously, Kevin was the Regional President for TD Bank's Florida market; overseeing retail, consumer, commercial & middle market lending, government banking, and cash management. His former roles include Market President for Metro D.C., New York, New Jersey and Pennsylvania.

Prior to joining TD Bank, he was a member of Summit Bank's senior leadership team for 19 years and was the Regional President for the bank's New Jersey business.

He was appointed by former Florida Governor Scott to the Enterprise Florida Board. He was on the board for The Broward Workshop and the Florida Bankers Association.

He was a member of SHRM and the Sarasota / Manatee SHRA Chapter; College Relations Chair, board member for Family Success Institute and a pre-IPO mortgage service firm. He is Chair for Jesus Father of the Poor Clinic – Haiti. He is an advisory board member for the business and accountancy school at State College of Florida.

He served in numerous New Jersey, Virginia and Washington DC based community organizations as board and chair roles.

Kevin graduated Lycoming College - BA in Business Administration, Sociology & Anthropology.



Mary Harrington

Symposium Moderator

Treasury & Payment Solutions

Synovus

Mary is a Senior Technical Consultant with the Treasury & Payment Solutions team at Synovus Bank. She has over 30 years of Banking, Payments Technology and Treasury Management experience including Sales Management, Product Development, Training, and Payables/Receivables solution consulting. Her passion is helping clients by sharing insights on the latest fraud trends and best practices in mitigation strategies. She works closely with the Synovus Fraud and Financial Crimes Unit teams to stay abreast of the critical issues impacting both the Bank and our clients. She has been a frequent Cybersecurity speaker in Florida for events including the Florida Government Finance Officers Association (FGFOA), Florida Bar Association and Association for Financial Professionals (AFP). Mary has a B.S. in Finance from Miami University and is a Certified Treasury Professional.



Serge Jorgensen

Founding Partner and Chief
Technology Officer, Sylint Group

Serge Jorgensen is a founding partner and Chief Technology Officer in the Sylint Group, and provides technical development and guidance in the areas of Computer Security, Counter CyberWarfare, System Design and Incident Response. Mr. Jorgensen is a patented inventor in engineering and security-related fields, has held various security clearances and works closely with the FBI, DHS and others in tasking, analyzing and managing Information Security needs to safeguard critical infrastructure, manufacturing and other operations.

Sylint

Sylint provides leading edge expert services in Cyber Security, Digital Data Forensics, and eDiscovery. Formed in 1998, our firm has developed a national reputation as a leader in its field, and works internationally with Fortune 50 organizations to small firms and municipalities. Sylint is one of the few Payment Card Forensic Investigation and NSA-accredited Incident Response companies, with experience from National Intelligence Agencies, Department of Defense, law enforcement, and corporate entities used to provide comprehensive cyber security and investigative services. Services include detection and remediation of corporate espionage, fraud identification, cyber security posture review, and regulatory compliance.



Byron Shinn

CPA and Engagement Partner,
Carr Riggs & Ingram, CPA, LLC

Experience

Mr. Shinn is a partner in the Bradenton/Sarasota Region with over 38 years of public accounting experience. Byron leads and provides professional and responsive services in the areas of auditing, internal audits accounting, taxation and business consulting. Byron started Shinn & Co. in 1993 and merged into CRI in 2018. Prior to starting Shinn & Co, Byron worked for both local CPA firms as well as Arthur Andersen. Byron is very active with the Florida Board of Accountancy, having held positions as a member of the Probable Cause Panel (15 years) and Chair of the Board. Byron is on the Board of Trustees for the University of South Florida and a board member of the Sarasota Economic Development Council. Prior involvement has included past Chairman of the Florida Board of Accountancy, President of the Manatee Chamber, Past President of Kiwanis Club of Bradenton, Past Board Member of United Way of Manatee County, just to name a few.

Education, Licenses & Certifications

- B.A. University of South Florida, June 1979, Major in Accounting
- A.A. Manatee Junior College, June 1977
- CPA, State of Florida

Professional Affiliations and Organizations

- * American Institute of Certified Public Accountants (AICPA)
- * AICPA – Tax Practice & Procedures Committee
- * Florida Institute of Certified Public Accountants (FICPA)
- * Institute of Internal Auditors member
- * Bradenton Blue Foundation, Board member
- * EDC Sarasota, Board member
- * EDC Bradenton Area EDC
- * Florida Maritime Museum, Treasurer
- * University of South Florida, Trustee
- * Appointed to Florida Cybersecurity Task Force



Daniel Krug

Business Advisor, Northwest
Region Cybersecurity
Program Manager

FloridaMakes

Daniel is a 22 year veteran of the United States Air Force. He served most of his career in the RF Transmissions Systems and Cyberspace Support career fields. He also served in positions including Munitions Maintenance, Air Force Recruiter, Maintenance Control and Production, and Quality Control and Inspection. As a manager, he exercised control and leadership of a multi-organizational inspection team where he led in-depth management, safety, and compliance inspections. During his last four years of active duty, he served as an Instructor, Instructor Supervisor, and Element Chief at the Air Force's Technical Training School located at Fort Gordon, GA.

After retiring from the Air Force, Daniel worked for the University of West Florida in the Information Technology Academy as a Technical Coordinator and Instructor, teaching or assisting with CompTIA's A+, Network+ and Security+ programs, and Microsoft Windows 7 and Microsoft Certified Solutions Associate (MSCA) Windows Server 2012 program.

Daniel has a bachelor's degree from Tarleton State University with honors, Magna Cum Laude, in applied science, with a concentration in computer information systems. He has completed 33 of 36 hours towards a master's degree in information systems.

Daniel is the FloridaMakes Cybersecurity Program Manager and can help you understand cybersecurity and the new Department of Defense requirements as it relates to DFARS 252.240-7012, NIST 800-171 and the Cybersecurity Maturity Model Certification. Daniel also participates in the National Institute of Standards and Technology Manufacturers Extension Partnership (NIST MEP) National Network Cybersecurity Working Group.



Alfred Saikali

Chair, Privacy & Data Security
Practice

Shook Hardy & Bacon, LLP

Al Saikali is a national leader in privacy and data security law according to *Chambers* and *Legal 500*. Al represents companies in matters involving the collection, use, storage, and security of personal information. Al and his team at Shook Hardy & Bacon have represented companies in more than 150 privacy and data security class action lawsuits, including more biometric privacy class actions than any other law firm in the United States. He has represented companies in incident response matters impacting as many as ten million individuals in 120 countries. Al's dedication to his clients earned him the *Lexology* Client Service Award two years in a row.

In addition to chairing Shook Hardy & Bacon's Privacy and Data Security practice, Al founded and is Chair Emeritus of the Sedona Conference's Working Group on Privacy and Data Security Liability. He is one of a small number of data privacy practitioners who hold the Fellow in Privacy designation, accredited by the International Association of Privacy Professionals. Al is often quoted by the *Wall Street Journal*, *Bloomberg BusinessWeek*, and *Law360* for his thoughts on cybersecurity and data privacy trends.

In his spare time, Al maintains a blog (DataSecurityLawJournal.com), where he writes about emerging developments in privacy and data security law.



Andy Sekela

Special Agent, Private Sector
Coordinator

Federal Bureau of Investigation

SA Sekela graduated from the U.S. Naval Academy and served on the USS Batfish, a nuclear-powered attack submarine. SA Sekela completed a five-year tour with the Navy, and then worked in the private sector for seven years. After joining the FBI, SA Sekela spent five years at the Washington Field Office (working public corruption and government fraud investigations) and three years assigned to the International Corruption Unit at FBIHQ. SA Sekela is currently assigned to FBI Tampa. For seven years, he supervised a squad of Special Agents, Forensic Accountants, and Intelligence Analysts responsible for investigating white collar crime. He is currently assigned as the Private Sector Coordinator. In this role, he is responsible for liaison between the FBI and all non-government entities (including companies, financial institutions, and colleges/universities) in the 18 counties which make up the territory of the FBI Tampa Division.



Marc Schein, CIC, CLCS

National Co-Chair, Cyber Center
of Excellence

Marsh & McLennan Agency

Marc D. Schein, CIC, CLCS assists clients by customizing comprehensive commercial insurance programs that minimize or eliminate the burden of financial loss through cost effective transfer of risk. By conducting a Total Cost of Risk (TCoR) assessment, he can determine any gaps in coverage. As part of an effective risk management insurance team, Marc collaborates with senior risk consultants, certified insurance counselors, and expert underwriters to examine the adequacy of existing client programs and develop customized solutions to transfer risk, improve coverage and minimize premiums.

Marc is a seasoned Certified Insurance Counselor with experience working in multiple industries, including Cyber Security, Technology, Retail, E-commerce Financial Institution, Healthcare, Accounting and Law, among others. His risk management experience includes: Cyber Security, Cyber Insurance, Technology E&O, Directors and Officers, Employment Practices Liability, Errors & Omissions, Property, Casualty, Crime, Auto, and Workers' Compensation.

In 2011, Marc achieved his Commercial Lines Coverage Specialist (CLCS) designation. In 2014, he received his Certified Insurance Counselor (CIC) designation and was appointed to the Ponemon Institute's RIM Council (the pre-eminent research center dedicated to data protection, privacy and information security). In 2015, he was asked to join the Claims & Litigation Management Alliance's Cyber Committee. In 2017 Marc was appointed Northeast Cyber Champion for Marsh & McLennan Agency. A sought-after speaker and panelist on Data Breaches and Cyber Security, Marc has spoken before members of Congress and leaders in the Aviation Industry on Capitol Hill regarding the issues and costs of cyber breaches, and how to properly transfer risk to ensure that an organization or business is properly protected from what might otherwise be financially devastating recovery costs. He is also a co-founding member of Clean Machine Charity and Founder of a Nassau County-based networking group. He also founded a NYC think-tank roundtable for upper middle market trusted advisors to share complex challenges and solutions their clients face. Marc also maintains membership in Business Networking International. A graduate of SUNY Oneonta, Marc was a Business Economics Major and Communications Minor who made Dean's List.