The Cyber Security Symposium Series

Preparing for the worst: Key features of a cyber security incident response plan

February 24, 2021

Presented by

SYNOVUS® the bank of here

CRI CARR RIGGS & INGRAM CPAs and Advisors

Sylint Cyber Security, Incident Response & Digital Data Forensics

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

Michelle Schauerman

Breach Response Services Manager – Cyber & Executive Risk,

Beazley Group

Joseph W. Swanson

Attorney at Law

Carlton Fields

Paul Vitchcock

Supervisory Special Agent,

Federal Bureau of Investigation

Serge Jorgensen

Founding Partner and Chief Technology Officer,

Sylint Group

Byron Shinn

CPA and Engagement Partner

Carr Riggs & Ingram, CPA, LLC

If a cyber breach were to happen at your company:

Who would you call?

- Attorney
- Bank
- IT Specialist/Company
- Insurance Agent
- Corporate Security
- Risk Team
- CEO or COO
- Technical Services
- Company Owner
- Fraud Team
- Bank's Wire Department
- Police
- My Supervisor
- Network Engineers
- Local Authorities
- Not sure
- It Depends…

Cyber Insurance 101

Michelle Schauerman

beazley

Cyber Insurance 101

- ❑ Cyber risks are insurable!

- ❑ Cyber risk includes:

  - Privacy risk
  - Security risk
  - Operational risk

- ❑ Who is at risk?

  - Any business that stores sensitive data (PII, PHI, PCI)
  - Any business that is susceptible to business interruption due to cyber events (i.e. reliant on technology, hardware, software, cloud services, third party providers, etc.)

- ❑ Cyber incidents are on the rise!

beazley

What is covered?

- Coverage and limits vary drastically across the industry
- Common coverage elements include:

Breach Response Services

- ✓ Forensics
- ✓ Legal
- ✓ Crisis Management/Public Relations
- ✓ Ransomware negotiation
- ✓ Notification Vendors
- ✓ Credit Monitoring

First Party Coverage

- ✓ Business interruption
- ✓ Data Recovery
- ✓ Cyber Extortion
- ✓ eCrime

Third Party Coverage

- ✓ Regulatory defense and penalties
- ✓ Media liability
- ✓ Payment card liability

beazley

Sample Policy Limits & Retentions

CLAIM	LIMIT	RETENTION
Aggregate Limit	$2,000,000	-
Breach Response Services	$1,000,000	$5,000
Notification	100,000 notified individuals	100 notified individuals
Business Interruption Loss	$2,000,000	$10,000
Cyber Extortion Loss	$2,000,000	$10,000
Data Recovery Costs	$2,000,000	$10,000
Liability (data, regulatory, media)	$2,000,000	$10,000
eCrime (fraudulent instruction, fund transfer fraud)	$250,000	$10,000

beazley

Cyber Insurance Applications

- Ransomware has drastically changed the approach to underwriting.
- Historically, applications focused on 20+ generic cyber underwriting questions.
- Today, underwriters base their decisions on control measures and utilize a ransomware application, tailored at identifying an organization's preparation.
- Underwriters want to follow the ransomware kill chain based off:
    - Email Security
    - Internal Security
    - Back-Ups
    - Recoveries
- Clients with poor controls will receive less favorable terms and risk being deemed uninsurable depending on all factors.

beazley

Trends

- Ransomware
    - Increased activity
    - Increased demands
    - Exfiltration is common
    - New variants identified regularly
- Fraudulent instruction
    - As of September 2020, fraudulent instruction incidents targeting the middle market increased from 24% to 55%
    - Targets: healthcare, financial institutions, manufacturing, real estate, and education
- Sophisticated middle market attacks
    - As of September 2020, middle market attacks increased from 46% to 60%
    - Resiliency during the pandemic
    - Richer targets
- SolarWinds Orion

beazley

Cases

Industry	Cause of Breach/ Claim	Description
Financial Services	Payment card fraud Data breach	A credit union discovered malware on the majority of its computers. The credit union's HR director's account was accessed, and money was electronically transferred from a bank account. All 140,000 members were notified and offered credit monitoring. Insurance breach response services coordinated the response which included panel legal, forensic, notification, call center and credit monitoring services.
Higher Education	Hacking or malware Data breach	A university employee's computer became infected with malware, and the computer contained PHI and PII. Before the insurer was notified by the university, forensic evidence was wiped in a routine cleanup by IT. The university also retained an off-panel forensics firm which concluded that no information was compromised. The university decided to get a second opinion, and insurance breach response services arranged for a forensics firm to investigate. The panel forensics firm reviewed documents and salvageable data, and with the help of panel counsel, determined the need to notify and offer credit monitoring to 12,000 individuals.
Retail	Cyber Extortion	After a DDoS attack that forced an online retailer to take down its website, the retailer received a demand from the hacker for several thousand dollars in Bitcoin, threatening a larger DDoS attack if the retailer did not pay. Rather than pay the monetary demand, the retailer purchased upgraded DDoS protection services in response to the threat. Insurance paid over $60,000 in cyber extortion loss.
Technology Services	Data Breach	An international software company suffered a malware attack affecting dozens of servers, desktops and laptops. The company incurred significant amounts in external forensic costs investigating the scope and impact of the attack, recovering data and restoring impacted systems. Insurance reimbursed the company over $800,000 in data protection loss and privacy breach costs.

beazley

Additional Benefits

Some carriers offer added benefits for policyholders

- Workshops & Training
    - Information Security Best Practices
    - Incident Response
    - Business Continuity Planning
- Discounted Pre-Breach Services
    - Ransomware assessments
    - Vulnerability and penetrating testing
    - IRP development
- Post-Breach Services

beazley

1

Latest Threats and Case Studies

CARLTON FIELDS

Ransomware: The Latest Scourge

- **What is it?**
  - Malware that locks files and systems
  - May involve data exfiltration, too

- **What are the different types?**
  - Ryuk, CryptoLocker, Egregor, Sodinokibi

- **Massive increase in attacks**
  - COVID-19 boom, threat actors “renting” malware

- **Risk of Treasury enforcement**
  - Sanction violations
  - SAR filing obligation

CARLTON FIELDS

Ransomware Incident Response: *Order of Operations*

Phase 1	**Intake**: Learn of the incident
Phase 2	**Internal team**: Assemble incident response team
Phase 3	**External team**: Insurance reporting, then hire as needed, in this order: counsel, forensics, threat actor engagement, rebuild team, media relations.
Phase 4	**Systems work**: Threat actor engagement Assess backups Clean and harden
Phase 5	**Pay or don't pay**
Phase 6	**PII review**: Assess personal information and notice
Phase 7	**Post-mortem**

CARLTON FIELDS

Business Email Compromise: *A Growing Epidemic*

- Scam involving compromised or "spoofed" email accounts
  - Use of social engineering and/or computer intrusion
  - Targeting wire transfers
  - Foreign bank accounts – China, Hong Kong, UK, Mexico, Turkey
    - Domestic money mules
- In 2019, FBI's IC3 received 23,775 BEC complaints
  - Losses of over $1.7 billion
  - That is more than double the losses from 2017
- Growing sophistication
  - Fraudulent verification
  - Artificial intelligence/machine learning – spoofed voices

CARLTON FIELDS

Business Email Compromise: *Who pays?*

- Unsettled law with a variety of legal theories:
  - Negligence
  - Breach of Contract (written or implied)
  - Breach of Fiduciary Duty
  - Violation of Consumer Protection Act
- Most claims settle without a determination of liability
- Best practices
  - Assume a duty exists
  - Educate, train, and communicate
  - Show your work
  - Watch what you say (i.e., don’t over-promise)

CARLTON FIELDS

COVID-19: *Work From Home Risks*

- Rapid incorporation of new technologies
- New methods and types of data being collected and transferred
- Increased reliance on technology, increases hackers' opportunity and leverage
- Distracted employees
- Weaknesses in employees' home networks and computers
- Increasing number of attacks
  - Phishing
  - Business email compromise
  - Malware, including ransomware
- Company files getting lost in the mail

CARLTON FIELDS

2

Best Practices for Preparation and Response

CARLTON FIELDS

Make an Initial Assessment

1

- **Intake** of the potential **security event**
- Determine the nature of the event:
  - Vulnerability?
  - Breach with access?
  - Breach with acquisition?
  - System unavailability?
  - Impact critical infrastructure operations?
- Determine the **type of information** that may have been exposed
- Locate the **incident response guide** and begin the process

CARLTON FIELDS

Assemble the Incident Response Team (Internal)

- Legal
- Executive
- CISO
- Media Relations
- HR
- Business Unit
- Risk Manager
- IT Lead
- Customer Relations

CARLTON FIELDS

Who Helps the Incident Response Team (External)?

- Early on:
  - Insurance broker
  - Insurance carrier
  - Counsel
  - Forensics experts
  - Breach coach
  - Banking partners
- A little later:
  - Law enforcement
  - Public relations pros
  - Credit monitoring
  - Call centers / mailing houses

Start Investigation and Mitigation

- Reassess the initial assessment with the full team
- Determine if the breach is active
- Identify all affected systems, computers, and devices
- Identify the data, if any, at issue
- Interview key personnel
- Determine the cause of the breach
- Deploy technical mitigation efforts
- Determine when systems can be brought back online
- Use alternative communication channels as needed

Preserve Records of the Breach and Mitigation

- Preserve evidence of the breach, including log files
- Control the creation of new documents and records
- Document all efforts to investigate and mitigate the breach
- Involve the legal department and outside counsel as necessary, which may help to preserve the attorney-client and work product privileges

Determine Legal Notification Obligations

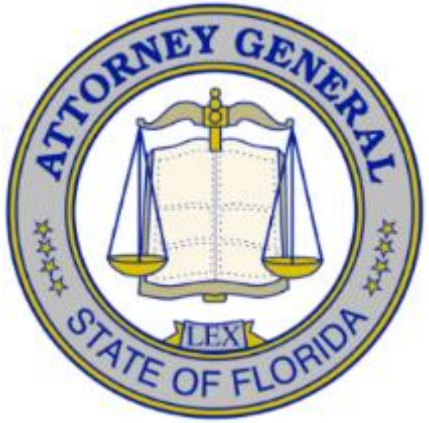
- Law enforcement
- State attorneys general
- Impacted customers or employees
- Acquiring bank and card brands (for credit card breaches)
- Regulators
- Credit reporting agencies
- Contract partners (if required by contract)

The Typical Data Security Statute (Florida)

- "Each covered entity … shall take **reasonable measures** to protect and secure data in electronic form containing personal information."
- "'Breach [ ]' means **unauthorized access** of data in electronic form containing **personal information** … ."
- No focus on privacy, just data security and notice.

- If there is a breach, a company must provide **notice**:
  - "to each individual **in this state** whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach."
  - "as expeditiously as practicable and without unreasonable delay . . . but no later than **30 days** after the determination of a breach or reason to believe a breach occurred."
  - to the Attorney General if **500 or more** Floridians.

Interacting with Law Enforcement



CARLTON FIELDS

Make this question part of your incident response plan

If NOT required, consider factors against outreach:

- Possible liability
- Disruption of business
- Possibility of increased publicity
- Confidentiality concerns

Compelling reasons in favor of outreach:

- LE might be notified anyway
- Benefit from LE's tools and relationships
- Manage the situation
- Mitigate liability
- Delayed public notification
- Deterrent effect

Tips for Working with Law Enforcement

- **Identify a single point of contact for law enforcement**
  - Speeds communication with LE
  - Task with “chain of custody” and big picture
- **Interview IT and other knowledgeable staff**
  - Identify witnesses
  - Identify sources of evidence
- **Preserve the evidence**
  - IP logs, system access, suspicious calls/emails
  - Cease routine overriding of data
- **Draft a “prosecution memo”**
  - Lays out the crimes, evidence, and other factors
  - Agents will use it as a roadmap when talking to prosecutor

4

Practical Tips

CARLTON FIELDS

Security Strategies

Privileged access management

Security settings

Threat identification and response

Data protection and encryption

Social engineering awareness

CARLTON FIELDS

Tools & Terminology

- Mail Filter (e.g., ProofPoint, Mimecast, BlueCoat)
- Endpoint Detection & Response (e.g., CarbonBlack, Microsoft ATP, Sophos)
- Next Generation Firewalls (e.g., PaloAlto, CheckPoint, Meraki)
- Vulnerability Scanning (e.g., Tenable, Rapid7)
- Centralized Logging (e.g., Sentinel, Splunk)
- Multifactor Authentication (e.g., Duo, Okta, Authenticator)

Key Takeaways

- Have Insurance
- Have an Incident Response Plan in place
- Don’t retain data – Subject to litigation preservation
- Provide suitable tools
- Conduct a Risk Assessment
- Train your team
- Don’t trust emails
- Make & Test Backups
- Know where your data is

Lessons Lost

Florida Cyber Security Update

Florida Task Force – Byron Shinn

- The Governor established a Cybersecurity Task Force , chaired by the Lt. Governor, to make recommendations which would be forwarded to the 2021 legislative session for enactment.
- This legislation will probably be effective in 2021. This new legislation will be broad and far reaching with Florida's 37 Agencies and potentially certain supply chain vendors.
- A few of the key objectives were -
  - Recommend methods to secure the state's network systems and data, including standardized plans and procedures to identify developing threats and to prevent unauthorized access and destruction of data.
  - Recommend a process to regularly assess cybersecurity infrastructure
  - Review of cyber infrastructure and recommendations for improvement
  - Review of operating plans for the response, coordination and recovery from a cybersecurity incident.

Summary of findings sent to the Governor, Senate President and Speaker of the House by February 1, 2021, which was completed

What resources are available to help

Take advantage of the resources and information that is available

- 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
- 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

Q&A

Michelle Schauerman

Breach Response Services Manager-

Cyber & Executive Risk, Beazley Group

michelle.schauerman@beazley.com

Joseph W. Swanson

Attorney at Law, Carlton Fields

JSwanson@carltonfields.com

Paul Vitchock

Supervisory Special Agent,

Federal Bureau of Investigation

pjvitchock@fbi.gov

Serge Jorgensen

CTO, Sylint Group

sjorgensen@sylint.com

Byron Shinn

Partner, Carr Riggs & Ingram

bshinn@cricpa.com

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.

SYNOVUS®
the bank of here

CRI CARR RIGGS & INGRAM
CPAs and Advisors

Sylint
Cyber Security, Incident Response & Digital Data Forensics

Appendix

SYNOVUS®
the bank of here

CRI CARR RIGGS & INGRAM
CPAs and Advisors

Sylint
Cyber Security, Incident Response & Digital Data Forensics

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

Michelle Schauerman

Breach Response Services Manager – Cyber & Executive Risk

Beazley Group

Michelle currently works as a Breach Response Services Manager with Beazley Insurance, where she assists insureds in their response to cyber and privacy incidents. Prior to joining Beazley, Michelle worked as a compliance analyst for a reinsurer and also spent ten years working in insurance and estate planning at a private wealth management firm.

Michelle graduated with B.B.A. in Finance and Real Estate from Temple University's Fox School of Business and is currently enrolled at the Drexel University Thomas R. Kline School of Law to obtain an M.L.S. in Cybersecurity and Information Privacy Compliance. She also maintains professional designations as a Chartered Life Underwriter (CLU®) and a Chartered Financial Consultant (ChFC®).

Joseph W. Swanson

Attorney at Law

Carlton Fields

Joe Swanson, chair of Carlton Fields' cybersecurity and privacy practice, advises clients on a variety of issues related to cybersecurity and privacy. He investigates and responds to data breaches and similar cyber incidents—including in the insurance and financial services industries, and he defends clients in litigation stemming from those incidents. In addition, Joe advises on best practices for interacting with law enforcement, regulators, and other constituencies in the event of a cyber incident. Joe also assists clients with drafting incident response guides and related cyber policies and procedures, as well as complying with privacy laws and regulations, such as the EU General Data Protection Regulation and the California Consumer Privacy Act.

In addition to Joe's cybersecurity and privacy practice, he represents companies and individuals in government and criminal investigations and conducts internal investigations. Joe also defends companies, executives, and directors in shareholder litigation and high-stakes commercial litigation in federal and state court.

Before joining Carlton Fields, Joe served as an assistant U.S. attorney in the Criminal Division of the U.S. Attorney's Office for the Middle District of Florida. In that role, Joe served as the office's Computer Hacking and Intellectual Property Coordinator.

Paul Vitchcock

Supervisory Special Agent

Federal Bureau of Investigation

Supervisory Special Agent Paul J. Vitchock currently manages the FBI Cyber Squad in Tampa and Orlando which includes criminal and national security investigations. SSA Vitchock investigated computer intrusion matters in Pittsburgh and Washington, DC, managed the FBI Eurasian Organized Cyber Crime program at FBIHQ, and most recently served as the FBI Cyber Attaché at the US Embassy in Bucharest, Romania. SSA Vitchock was also a member of the FBI SWAT teams in Pittsburgh and Washington. Before joining the FBI, SSA Vitchock spent nine years in the Washington D.C. area working as a network infrastructure and security consultant and manager.