The DNA of Cybersecurity Risks

Presented by: Doug Roossien, CRM, CFE
Business Protection Risk Management
CUNA Mutual Group

CUNA MUTUAL GROUP

Common Purpose. Uncommon Commitment.

Data Breaches – How do they Happen?

- Network hackers and malware
- Employee negligence/theft
- Lost/stolen laptops, backup tapes/disks and other data-bearing mobile devices
- Vendor leaks/mistakes

Data Breaches

- Financial risk
- Compliance/Legal risk
- Reputation risk

A data breach can result in more than lost data. It can damage the credit union's reputation, shake member trust, and cost tens of thousands to repair.

Agenda

- Data breach studies by the Ponemon Institute, Mandiant, BakerHostetler and Verizon
- Malware's role in data breaches
- Data breach insurance claims study – NetDiligence
- Best practices for securing members' confidential data
- Mobile devices
- Incidence response planning

Incident Response Planning: The Good, The Bad and The Ugly

The Good

- 81% have an incident response plan in place compared to 73% in last year's study

The Bad

- 35% say they have not reviewed or updated their incident response plan since it was put into place
- 45% say they do not practice responding to a data breach or waits more than 2 years to practice
- Only 57% have training and security awareness programs

The Ugly

- Only 34% say they are effective or very effective in developing and executing their incident response plan
- Only 39% say they are prepared to respond to a breach of confidential information/intellectual property
- Only 36% say they know what needs to be done in responding to a material data breach to prevent loss of customer trust

Source: Ponemon Institute's 2015 study, Is Your Company Ready for a Big Data Breach?

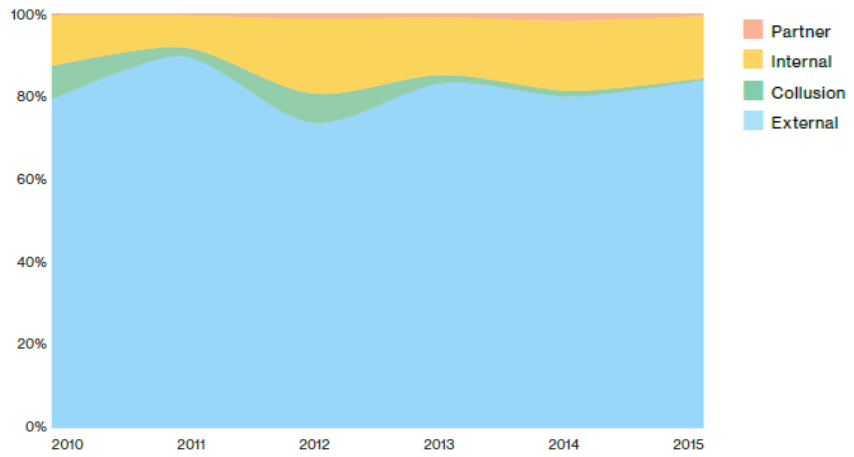
Mandiant M-Trends Report Findings

Self-detection is on the rise and the timeliness of detection is improving.

Year	How Compromises were Discovered		Median # of Days From Earliest Evidence of Compromise to Date of Discovery
	External Party	Internally	
2012	94%	6%	416
2014	69%	31%	205
2015	53%	47%	146

Source: Mandiant M-Trends Reports

Verizon 2016 Data Breach Investigations Report



External threats far exceed internal threats and partner threats.

Source: Verizon 2016 Data Breach Investigations Report

Verizon 2016 Data Breach Investigations Report

Malware is distributed in phishing attacks

- Combined over 8 million results from sanctioned phishing tests in 2015 by security awareness vendors
- 30% of phishing messages were opened by the recipients
- ~12% clicked on the malicious attachment or link to malicious website

Think before you click!

Source: Verizon 2016 Data Breach Investigations Report

Verizon 2015 Data Breach Investigations Report

Malware is distributed in spear phishing attacks

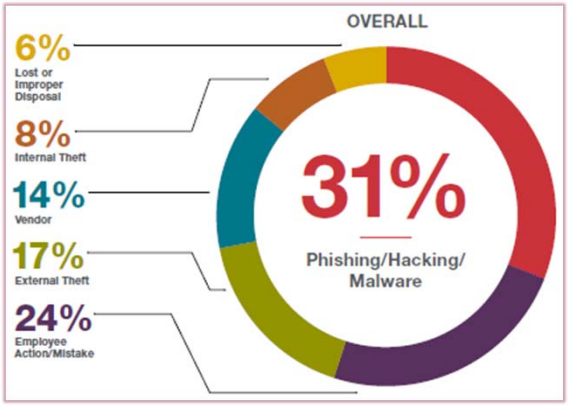
- Aggregated the results of over 150,000 emails sent by two security awareness partners in a controlled study
- 50% of the recipients opened the email and clicked on the link within the first hour

Think before you click!

Source: Verizon 2015 Data Breach Investigations Report

Phishing, Hacking & Malware

- Phishing, hacking & malware were the top cause in all incidents the firm helped manage in 2015 – 31% (**36% in financial services industry**)
- Many of the underlying issues that enabled phishing/hacking/malware incidents could be attributed to human error



Source: BakerHostetler 2016 Data Security Incident Response Report

Malware's Role in Data Breaches

- Data breaches are frequently the result of credential-stealing malware
- Distributed in spear phishing attacks
- Tool of choice in Advance Persistent Threat (APT) attacks

Think before you click!

Stages of an APT Attack

Step	Description
1. Intelligence gathering	Attackers identify and gather publicly available information on the targeted organization. The goal is to obtain important information on the organization's IT environment and organizational structure.
2. Point of entry	Attackers deploy spear phishing campaigns against key employees of the targeted organization. The goal is to infect the network with malware
3. Establish communication with C&C	Once planted on the network, the malware establishes communication with the attackers command & control (C&C) center to deliver information, receive instructions and download additional malware.
4. Lateral movement through network	Once inside, the attackers move slowly across the network to avoid detection searching for sensitive data to steal and the credentials necessary to access that data.
5. Data discovery	By downloading tools through the C&C, the attackers scan the network to identify specific servers and systems where sensitive data is located.
6. Data exfiltration	Attackers transmit the sensitive data out of the network to external locations. Encryption and other techniques are commonly used to disguise the data transmissions.

APTs are to intrusion detection what stealth aircraft are to radar

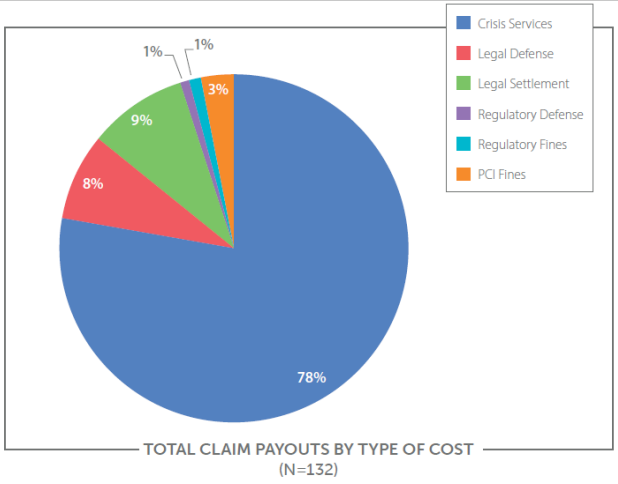
NetDiligence
2015 Cyber Liability & Data Breach Insurance Claims

- Per breach costs
  - Average payout: $673,767 — Median payout: $76,984
- Per record costs
  - Average cost per record: $964.31 — Median cost per record: $13.00
  - Average records lost: 3.2 million — Median records lost: 2,300
- Crisis service costs
  - Average cost of crisis services: $499,710 — Median cost of crisis services: $60,563
  - Crisis services include the cost of forensics, legal counsel guidance, notification and credit monitoring
- Legal costs
  - Average cost of legal defense: $434,354 — Median cost of legal defense: $73,600
  - Average cost of settlement: $880,839 — Median cost of settlement: $50,000

Source: NetDiligence 2015 Cyber Liability & Data Breach Claims Study

NetDiligence
2015 Cyber Liability & Data Breach Insurance Claims

Of the $75.5 million in total claims reviewed, 78% was spent on crisis services.



Why the Problem?

- Intrusion detection and network monitoring is weak
- Lack of encryption
- Malware
- Websites are porous and need constant care
  - Hardening and patching
- Cyber thieves take advantage of human error
  - Unchanged default settings
  - Failing to install patches
  - Failing to protect laptops
  - Improper disposal of paper records
  - Weak passwords

Best Practices

Protect data wherever it is located

- ✓ **At rest**
- ✓ **In motion**
- ✓ **In use**

- Encryption
  - Data residing on the network (servers, workstation hard drives and laptops)
  - Data residing on mobile devices
  - Backup tapes/disks
  - Data transmitted over the Internet and in emails
- Firewall
- Up-to-date antivirus/antimalware protection
- Spam and web filters
- Intrusion detection system (IDS)/intrusion prevention system (IPS)
- Install operating system patches when made available

Best Practices

Protect data wherever it is located

- ✓ **At rest**
- ✓ **In motion**
- ✓ **In use**

- Vulnerability assessments
- Penetration testing
- Monitor system logs
- Lockdown workstation USB ports
  - Helps prevent insider theft of confidential member data
- Data loss prevention (DLP) solution
  - Identifies, monitors, and protects data at rest, in motion, and in use
  - DLP tools allow credit unions to see which databases, file servers, desktops and laptops hold sensitive data
  - Identifies when someone is transmitting data via email or downloading to external storage devices
- Third-party reviews of network security
- Secure paper records

Best Practices

Protect data wherever it is located

- ✓ **At rest**
- ✓ **In motion**
- ✓ **In use**

- Accessing network/systems remotely
  - Telecommuters working from home
  - Third-party vendors

Remote Access Best Practices

- Prohibit remote employees from using home computers to access network
- Establish a virtual private network (VPN)
  - A VPN is a network that uses the Internet to provide remote employees with secure access to the credit union's network
- Prohibit employees from using unsecure wireless networks (public Wi-Fi)
- Require multifactor authentication – not just usernames and passwords
  - One-time-password tokens
  - Plug-in tokens

Mobile Devices: Tablets / Smartphones

- Credit union issued versus employee use of personal devices (BYOD)
  - Both should be secured
- Secure the business side of the device (sandboxing)
  - Good Technology
  - MaaS360
- Adopt acceptable use policy

Mobile Devices Used for Business Purposes

- **Antivirus software**
- **Password protect the device/time-out feature to lock the device**
- **Remote wipe capability**
- **Prohibit employees from storing confidential member data to the device**
  - ✓ **If it is necessary to store such data on the device, the data should be encrypted**
- **Encrypt confidential member data transmitted in emails**

Data Breaches – Employee Negligence

- Credit union discovered malware on 124 workstation pc's
  - Malware captures screen shots
  - Social Security numbers, account information and transaction records for 115,000 members may have been compromised
- Credit union employee accidentally published a file on the credit union's public-facing website
  - File contained member names, addresses, Social Security numbers, account numbers and account passwords on 33,000 members
  - File was accessed 10 times before it was removed
- Credit union employee accidently emailed a spreadsheet to a member
  - Spreadsheet contained member names and account numbers on 18,000 members
- Credit union employee's laptop stolen from vehicle
  - Contained unencrypted sensitive data (names, addresses, SSN's and account numbers) on 45,000 members

Source: CUMIS Insurance Society, Inc. claims data (2013-2015)

Data Breaches – Vendor Negligence

- Credit union uses third-party vendor to mail monthly account statements
  - Members received their correct statements plus a portion of statements belonging to other members
- Credit union downloaded confidential member data to a thumb drive for their outside auditor
  - Auditor lost the thumb drive in a public park while watching son's football game
  - 14,500 members impacted

Source: CUMIS Insurance Society, Inc. claims data (2013-2015)

Security Awareness Training

- Must be addressed in the credit union's information security program
- All employees should receive training on at least an annual basis
- The goal is to change employee behavior to reinforce good data security practices

Training Topics

- IT security policies, procedures and practices
- Information security program
- Incident response plan
- Physical security of data center
- Workstation computers / laptops
- User passwords
- Social engineering
- Malware
- Encryption
- Email security

Regulatory Environment

- NCUA Part 748
  - Appendix A, Guidelines for Safeguarding Member Information
  - Appendix B, Guidance on Response Programs
- Fair and Accurate Credit Transactions (FACT) Act's Red Flags Rule
- Plastic Card Industry Data Security Standards (PCI DSS) v3.1 (section 12.10), if applicable
- HIPAA Security Rule (Section 164.308)

State Data Breach Notification Laws

- 47 states, District of Columbia and U.S. Territories
- Laws vary between jurisdictions
  - Expanded definition of "personal information"
  - Risk of harm
  - Notification time frame
- Most state laws contain a safe harbor provision if the personal information breached was encrypted

Planning and Responding

Incident Response Plan

- Written incident response plan to address incidents of unauthorized access to member information
- Required by NCUA
  (Rules and Regulations Part 748, Appendix B)
- Minimum requirements include:
  - Assess nature and scope of incident
  - Identify what member information systems and the member information breached
  - Take appropriate action to contain and control the incident to prevent further unauthorized access to or use of member information
  - Notify NCUA Regional Director or appropriate state supervisory authority
  - File Suspicious Activity Report, if needed
  - Notify appropriate law enforcement agency
  - Notify impacted members

Suggested Practices

- ❑ Activate incident response team
- ❑ Contain the breach
- ❑ Analyze the breach
  - ❑ Record all information relevant to breach
  - ❑ Who, what, when and how
  - ❑ Forensics*
- ❑ Contact breach coach / legal counsel specializing in privacy issues
  Can be done immediately after discovery
- ❑ Notify your cyber liability insurance provider of potential loss
- ❑ Notify regulator
- ❑ File Suspicious Activity Report, if needed
- ❑ Analyze legal implications
  - ❑ Identify federal, state and local laws / regulations impacted
  - ❑ State data breach notification and timing requirements

Update & test the plan annually

*** Have a pre-determined list of IT forensics firms available**

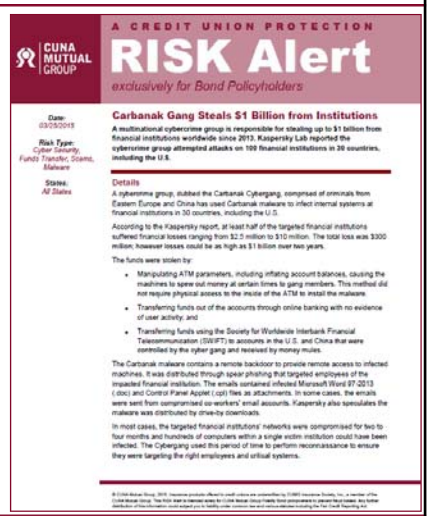
Malware – Beyond Theft of Data

Carbanak Malware

- Targeted 100 financial institutions in 30 countries, including U.S.
- Malware was distributed via phishing attacks
- Losses per institution ranged from $2.5M to $10M
- Funds stolen from institutions – not from depositor accounts
- Sought out employees with administrative rights
- Performed reconnaissance (video) to learn details of the 3rd party EFT systems used
- Logged into 3rd party EFT systems to transfer funds to other institutions

Think before you click!

Source: Kaspersky Lab, The Great Bank Robbery: The Carbanak APT



CUNA MUTUAL GROUP

A CREDIT UNION PROTECTION RISK Alert

exclusively for Bond Policyholders

Date: 03/25/2015

Risk Type: Cyber Security, Funds Transfer, Scams, Malware

States: All States

Carbanak Gang Steals $1 Billion from Institutions

A multinational cybercrime group is responsible for stealing up to $1 billion from financial institutions worldwide since 2013. Kaspersky Lab reported the cybercrime group attempted attacks on 100 financial institutions in 30 countries, including the U.S.

Details

A cybercrime group, dubbed the Carbanak Cybergang, comprised of criminals from Eastern Europe and China has used Carbanak malware to infect internal systems at financial institutions in 30 countries, including the U.S.

According to the Kaspersky report, at least half of the targeted financial institutions suffered financial losses ranging from $2.5 million to $10 million. The total loss was $300 million; however losses could be as high as $1 billion over two years.

The funds were stolen by:

- Manipulating ATM parameters, including inflating account balances, causing the machines to spew out money at certain times to gang members. This method did not require physical access to the inside of the ATM to install the malware.
- Transferring funds out of the accounts through online banking with no evidence of user activity; and
- Transferring funds using the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to accounts in the U.S. and China that were controlled by the cyber gang and received by money mules.

The Carbanak malware contains a remote backdoor to provide remote access to infected machines. It was distributed through spear phishing that targeted employees of the impacted financial institution. The emails contained infected Microsoft Word 97-2013 (.doc) and Control Panel Applet (.cpl) files as attachments. In some cases, the emails were sent from compromised co-workers' email accounts. Kaspersky also speculates the malware was distributed by drive-by downloads.

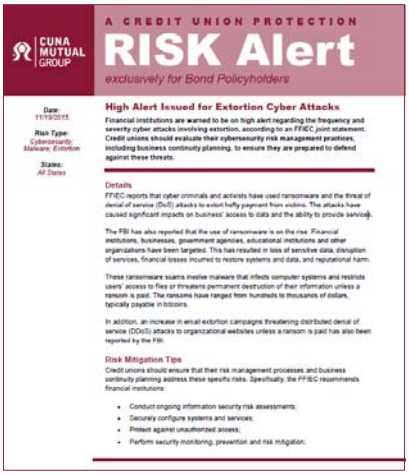
In most cases, the targeted financial institutions' networks were compromised for two to four months and hundreds of computers within a single victim institution could have been infected. The Cybergang used this period of time to perform reconnaissance to ensure they were targeting the right employees and critical systems.

Malware – Beyond Theft of Data

Ransomware

- The FBI reports an increase in ransomware (a form of malware)
- Encrypts sensitive files and deletes the originals
- Results in loss of sensitive data, disruption of services, financial losses incurred to restore systems and data, and reputational harm
- Restricts users' access to files or threatens permanent destruction of the information unless a ransom is paid

Think before you click!



CUNA MUTUAL GROUP

A CREDIT UNION PROTECTION

RISK Alert

exclusively for Bond Policyholders

Date: 11/13/2015

Risk Type: Cybersecurity; Malware; Extortion

States: All States

High Alert Issued for Extortion Cyber Attacks

Financial institutions are warned to be on high alert regarding the frequency and severity cyber attacks involving extortion, according to an FFIEC joint statement. Credit unions should evaluate their cybersecurity risk management practices, including business continuity planning, to ensure they are prepared to defend against these threats.

Details

FFIEC reports that cyber criminals and activists have used ransomware and the threat of denial of service (DoS) attacks to extort hefty payment from victims. The attacks have caused significant impacts on business' access to data and the ability to provide service.

The FBI has also reported that the use of ransomware is on the rise. Financial institutions, businesses, government agencies, educational institutions and other organizations have been targeted. This has resulted in loss of sensitive data, disruption of services, financial losses incurred to restore systems and data, and reputational harm.

These ransomware scams involve malware that infects computer systems and restricts users' access to files or threatens permanent destruction of their information unless a ransom is paid. The ransoms have ranged from hundreds to thousands of dollars, typically payable in bitcoins.

In addition, an increase in email extortion campaigns threatening distributed denial of service (DDoS) attacks to organizational websites unless a ransom is paid has also been reported by the FBI.

Risk Mitigation Tips

Credit unions should ensure that their risk management processes and business continuity planning address these specific risks. Specifically, the FFIEC recommends financial institutions:

- Conduct ongoing information security risk assessments;
- Securely configure systems and services;
- Protect against unauthorized access;
- Perform security monitoring, prevention and risk mitigation;

Malware – Beyond Theft of Data

Stolen login credentials to card processor's system*

- Malware (Trojan:Win32/Dynamer!ac) infected workstation PC at credit union
  - Card services employee's PC
- Compromised card services employee's login credentials to card processor's system by searching Internet browsing history
- Cyber thieves logged into card processor's system
  - Ordered 10 new debit cards
  - Removed daily dollar limits on the cards
  - Changed parameter so cards could be used outside of U.S.
- $200,000 loss

Think before you click!

* Source: CUMIS Insurance Society, Inc. claims data (2015)

Virus: Win32/Dynamer!ac

Virus:Win32/Dynamer!ac

Alert level: Severe

Summary | What to do now | Technical information | Symptoms

Threat behavior

We've automatically analyzed this threat, determined that it's a trojan because of what it does when it gets on a PC, and blocked and removed it from your PC.

Typically, trojans try to do one or all of the following:

- Download and install other malware.
- Use your computer for click fraud.
- Record your keystrokes and the sites you visit.
- Send information about your PC, including usernames and browsing history, to a remote malicious hacker.
- Give a remote malicious hacker access to your PC.

Due to the generic nature of this threat, we are unable to provide specific information on what it does.

Find out more about how we use machine learning to help guard against the latest malware threats:

- Windows Defender: Rise of the machine (learning)

Source: Microsoft

Don't Over-Promise & Under-Deliver

Increase in enforcement actions over misleading (deceptive) statements on data security practices

Details

- Federal Trade Commission (FTC) and Wyndham Worldwide Corporation
  - Massive payment card breaches in 2008 and 2009
  - FTC's action alleged the hotelier's privacy policy was deceptive
  - Wyndham's privacy policy stated, in part: "We safeguard our Customers' personally identifiable information by using *industry standard practices*"
- Consumer Financial Protection Bureau (CFPB) and Dwolla, Inc.
  - CFPB alleged Dwolla's website and communications misrepresented its data security practices by stating they met or exceeded industry practices
  - Used terms, "*exceeded industry standards*" and "*surpass industry security standards*"

Risk Mitigation

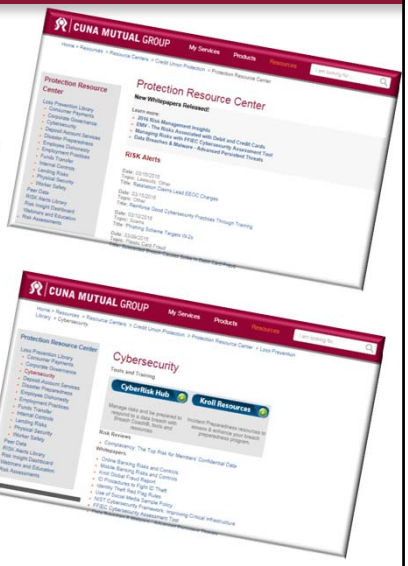
- Credit unions should review their privacy notice and marketing material to ensure they provide an accurate description of the policies and practices for protecting members' personal information
- Avoid implying your data security practices meet or exceed industry standards unless, for example, you receive certification from an accredited third-party that the credit union conforms to ISO 27001 (a well-known standard providing requirements for an information security management system), or similar standard

Session Summary

- Information theft is one of today's most common forms of fraud
- Given the financial, legal, and reputational risks of a data breach -- failing to prepare can be disaster

Protection Resource Center

- RISK Alerts
- White papers
  - Data Breaches & Malware – Advanced Persistent Threats
  - FFIEC Cybersecurity Assessment Tool
  - NIST Cybersecurity Framework
- Online risk assessments
  - Data and Network Security
- Cyber Insurance Policyholders can access
  - CyberRisk Hub & Kroll Incident Preparedness Resources (available to CUNA Mutual Group CSI Incident Package policyholders)
  - Beazley Breach Response Solutions (available to Beazley cyber policyholders)



Questions & Answers

Doug Roossien, CRM, CFE
Risk Management Consultant
CUNA Mutual Group
Email: douglas.roossien@cunamutual.com

CUNA MUTUAL GROUP

Common Purpose. Uncommon Commitment.

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/ publication, nor does it replace any provisions of any insurance policy or bond.

CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group. Some coverages may not be available in all states. If a coverage is not available from one of our member companies, CUNA Mutual Insurance Agency, Inc., our insurance producer affiliate, may assist us in placing coverage with other insurance carriers in order to serve our customers' needs. For example, the Workers' Compensation Policy is underwritten by non-affiliated admitted carriers. CUMIS Specialty Insurance Company, our excess and surplus lines carrier, underwrites coverages that are not available in the admitted market. Data breach services are offered by Kroll, a member of the Altegrity family of businesses. Cyber liability may be underwritten by Beazley Insurance Group.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.