MARYLAND GFOA FALL 2021 QUARTERLY CONFERENCE – LINTHICUM, MD

Cyber Security, Risk & Cyber Insurance Update

Local Government Insurance Trust (LGIT)
Scott Soderstrom
Director of Underwriting
www.lgit.org
scott@lgit.org
443 561 1729

BIO

Scott Soderstrom is Director of Underwriting at LGIT with 35 years in the insurance industry and 26 years with LGIT serving Maryland Local Governments. Graduated from George Mason University in 1986 with a B.S. in Business Administration and holds various insurance and risk management designations

(CPCU, ARM, ARME, ARMP)

LGIT BOARD OF TRUSTEES

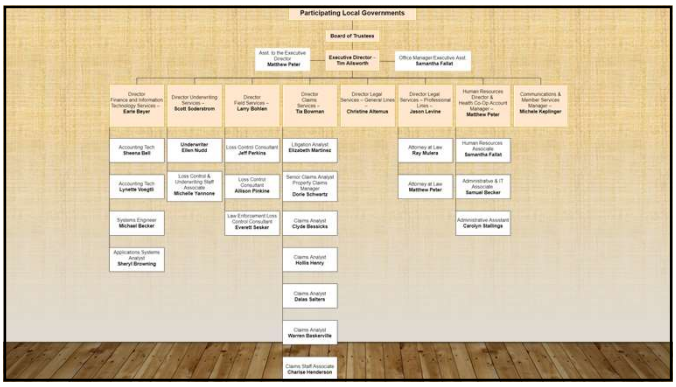
- John Miller, Chair, Middletown
- *Ted Zaleski, Vice Chair, Carroll County (MDGFOA)*
- Abigail McNinch, Secretary, Town of Denton
- Tracy Grant, Town of Edmonston
- Shelley Heller, Kent County
- Michael Sanderson, Ex-Officio, MACO
- *Eric Jackson, Charles County (MDGFOA Pres)*
- Emily Keller, City of Hagerstown
- Amy Lanham, Howard County
- Daniel Mears, City of Bowie
- John O'Connor, St. Mary's County
- Scott Hancock, Ex-Officio, MML

LGIT – LOCAL GOVERNMENT INSURANCE TRUST

LGIT is a non-profit risk pool owned and managed by its member local governments including the Maryland Municipal League and Maryland Association of Counties both created LGIT in 1987

LGIT MISSION

The Local Government Insurance Trust will provide coverage and risk management services at stable and competitive rates through an organization that is owned and managed by its local government members



RANSOMWARE

- Since 2016 – 4,000 ransomware attacks per day on average or 166 per hour
- CNA Insurance ransomware attack cost them $40M
- Avg ransomware fee - $200,000 in 2020
- Avg downtime – 21 days
- 80% who paid the ransom attacked again and 46% data retrieved was corrupted
- 33% cyber attacks on governments were ransomware
- FL city paid $600,000 ransom (Riviera Beach City)
- Only 38% local/state govt employees trained in ransomware prevention
- Ransomware cost New Orleans $7M
- 87th Conference of Mayors - 226 mayors in 40 states agreed never to pay a ransom

Source: Sobers, Rob, Varonis, 81 Ransomware Statistics, Data, Trends and Facts for 2021, 7/6/21, https://www.varonis.com/blog/ransomware-statistics-2021/

RANSOMWARE

- Atlanta didn't pay $51,000 ransomware; cost $17M to fix.
- Baltimore City didn't pay 13 bitcoins (ie. $75K); paid $18M to fix.
- 22 Texas municipalities didn't pay $2.5M ransom but MSP had good backups.
- Oldsmar, FL unsuccessful attack to poison water supply with sodium hydroxide in the water from 100 parts per million to 11,100 parts per million Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners. It is used to control water acidity and remove metals from drinking water in water treatment plants."

Sources: (Miller, Maggie, *THE HILL*, Hackers breach, attempt to poison Florida city's water supply, 02/08/21, https://thehill.com/policy/cybersecurity/537890-hackers-breach-attempt-to-poison-florida-citys-water-supply)

CYBER MARKET REPORT

- Cyber Insurance Market 2021 was terrible (Hard market again) and expected 2022.
- Premium increases 200-300% increases
- Less coverages, lower limits and higher deductibles
- Non-renewals – one MD county was non-renewed by major insurer who LGIT covered for FREE.
- Increased cyber attacks
- Commercial market abandoning Public Entities (like 1980s all over again with Police and Public Officials policies)
- COVID -working from home – increased vulnerability (lack of VPN, employee owned devices to the network, passwords, etc)
- Commercial insurers starting to use delay tactics in handling ransomware claims

CYBER THREATS TO LOCAL GOVERNMENTS

- Ransomware on critical infrastructure (Soft targets due to being underfunded, under-resourced, under-protected) including local governments via internet, removable devices and email clients.
  - SCADA & ICS (Supervisory Control and Data Acquisition & Industrial Control Systems)
  - Water & Sewer
  - Electric plants
  - 911telecommunication systems
  - Traffic
  - Airports
  - IOT
  - Smart Cities

Source: Cybersecurity & Infrastructure Security Agency (CISA) https://www.cisa.gov/water-and-wastewater-systems-sector

RANSOMWARE

- It's a business, an ecosystem – For profit ransomware groups (aka cyber criminal gangs, syndicates, franchise ops)
- REvil, Darkside, Nobelium, Conti, etc – typically Russian backed cyber criminal hacking groups (responsible for Colonial Pipeline, JBS, SolarWinds and Kaseya attacks) using or offering Ransomware as a Service (RaaS).[1]
- RaaS – A subscription turnkey software/service sold or rented on the dark web – a serious problem as anyone without any hacking skills can buy and not know how to provide a decryption key once in!- More prevalent than ever. (ie. be on ALERT!)[2]
- Triple Extortion Tactics: 1. Encryption, 2. Exfiltrate data for more leverage, 3. DDos Attacks for more leverage.[2]
- In May 2021, FBI and CISA (Cybersecurity and Infrastructure Security Agency) issued a joint alert for owners of critical infrastructure.
- To pay or not to pay, that is the question.
- Only 29% recover their files and just 8% got all their data back after paying a ransom according to cybersecurity companies Kaspersky and Sophos.

Sources: 1. Sobers, Rob, Varonis, 81 Ransomware Statistics, Data, Trends and Facts for 2021, https://www.varonis.com/blog/ransomware-statistics-2021/

2. Moorcraft, Bethan, The Rise of Triple Extortion in Ransomware Pandemic, Oct 25, 2021, https://www.insurancebusinessmag.com/us/news/cyber/the-rise-of-triple-extortion-in-ransomware-pandemic-314282.aspx?utm_source=GA&utm_medium=20211026&utm_campaign=IBAW-Cyber-20211026&utm_content=6A4B8BD6-A7CD-419D-9027-5133AF446A90&tu=6A4B8BD6-A7CD-419D-9027-5133AF446A90

GOOD NEWS

October
is
National Cybersecurity Awareness Month!

However,

A high attack month and Halloween (trick or treat?)*

Appears to correlate with holidays and natural disasters.*

Source: Sharma, Shweta, CSO, October is High Season for Cyberattacks, Infosec Institute Study Shows, 10/21/21, https://www.csoonline.com/article/3636161/october-is-high-season-for-cyberattacks-infosec-institute-study-shows.html

RANSOMWARE

Administrator Security Practices

Have multiple workable & tested backups. Basic tactic - 3-2-1-Rule

- Have at least three copies of their data,
- Store the copies on two different types of media
- Keep one backup copy offline or offsite

Updated Security software and update patches

Multi-factor authentication

Cloud Security

End Point User Security Practices

Email attachments or links – be careful

Avoid suspicious websites (https)

Train employees

Password management

CYBER INSURANCE

- Cyber policies started for most part in last 10-15 years with Breach Notification Laws in CA 2003.
- Insurance a cure-all? NO
- Loss prevention is a MUST with MFAs, backups, training, upgrades, patches, etc.
- However, Insurance as an important financial backup when (not if) loss control fails.
- Hard market in cyber insurance in 2021 & expected 2022?

- Currently, FREE Cyber Insurance for all LGIT Members with a limit of $2M with sublimits

SUMMARY OF CYBER INSURANCE COVERAGES

Main Coverage Components (Beazley Insurance Co. via Alliant Insurance)*

- Breach Response
- First Party (Property Insurance)
- Third Party (Liability Insurance)
- E-Crime
- Service Component – Access to specialists (IT, lawyers, PR, etc)

*This is only a summary of coverages. See policy for details which supersedes anything in these power point slides.

BREACH RESPONSE COVERAGE

Breach Response coverage

To indemnify Insured for Breach Response Costs incurred because of an actual or reasonably suspected Data Breach or Security Breach

BREACH RESPONSE COVERAGE

Breach Response Costs

- Attorney costs – evaluate obligations under Breach Notification Laws
- Computer security expert – determine existence, cause and scope
- Payment Card Industry (PCI) Forensics – investigate existence and extent of data breach involving payment card data and for a Qualified Security Assessor to certify PCI compliance required by your Merchant Services Agreement.
- Personal Identifiable Information (PII) notification costs
- Call Center costs
- Credit Monitoring, ID monitoring or other personal fraud or loss prevention solutions
- Public Relations costs

- **tmbclaims@beazley.com** & bbr.claims@beazley.com **& Claims@lgit.org**

BREACH RESPONSE COVERAGE

Data Breach

The theft, loss, or Unauthorized Disclosure of Personally Identifiable Information (PII) or Third Party Information that is in the care, custody or control of the Insured Organization or a third party for whose theft, loss or Unauthorized Disclosure of Personally Identifiable Information or Third Party Information the Insured Organization is liable.

BREACH RESPONSE COVERAGE

Security Breach

- Unauthorized Access or Use of Computer Systems, including Unauthorized Access or Use resulting from the theft of a password
- A denial of service attack affecting Computer Systems;
- Infection of Computer Systems by malicious code or transmission of malicious code from Computer Systems
- Regarding Liability, a denial of service attack to others

BREACH RESPONSE COVERAGE

Personally Identifiable Information

- Under state [MD] Breach Notice Law
- An individual's drivers license or state identification number, social security number, unpublished telephone number, and credit, debit or other financial account numbers in combination with associated security codes, access codes, passwords or PINs; if such information allows an individual to be uniquely and reliably identified or contacted or allows access to the individual's financial account or medical record information. but will not include information that is lawfully made available to the general public.

FIRST PARTY COVERAGE (PROPERTY)

- Business Interruption Loss
- Dependent Business Interruption Loss
- Cyber Extortion Loss (Ransomware)
- Data Recovery Costs
- Hardware Replacement Costs
- Reputation Loss

FIRST PARTY COVERAGE

Business Interruption Loss

- Loss of income/forensic expenses/extra expense resulting from a Security Breach or System Failure (water, sewer, electric, cable/fiber, etc)
- The voluntary and intentional shutdown of Computer Systems by the Insured Organization
- The intentional shutdown of Computer Systems by the Insured Organization as expressly required by any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity

FIRST PARTY COVERAGE

Dependent Business Interruption Loss

Loss of income/extra expenses from a Security Breach or System Failure (services from another town/county; major employers)

FIRST PARTY COVERAGE

Extra Expense

Reasonable and necessary expenses to minimize, reduce or avoid Income Loss, over and above those expenses would have incurred had no Security Breach, System Failure, Dependent Security Breach or Dependent System Failure occurred

FIRST PARTY COVERAGE

System Failure

An unintentional and unplanned interruption of Computer Systems

FIRST PARTY COVERAGE

Cyber Extortion (Ransomware)

Any Extortion Payment that has been made by or on your behalf
(with the Underwriters' prior written consent) to prevent or terminate an Extortion Threat

FIRST PARTY COVERAGE

Extortion Threat

- Alter, destroy, damage, delete or corrupt Data;
- Perpetrate the Unauthorized Access or Use of Computer Systems;
- Prevent access to Computer Systems or Data;
- Steal, misuse or publicly disclose Data, PII or Third Party Information:
- Introduce malicious code into Computer Systems or to third party computer systems; or
- Interrupt or suspend Computer Systems;

FIRST PARTY COVERAGE

Extortion Payment

Money, Digital Currency, marketable goods or services demanded to prevent or terminate an Extortion Threat.

FIRST PARTY COVERAGE

Digital Currency

- Requires cryptographic techniques to regulate the generation of units of currency and verify the transfer thereof
- Is both stored and transferred electronically
- Operates independently of a central bank or other central authority

FIRST PARTY COVERAGE

Data Recovery Costs

The reasonable and necessary costs incurred to regain access to, replace, or restore Data from a security breach

FIRST PARTY COVERAGE

Hardware Replacement Costs

Costs to replace computers or any associated devices or equipment operated by, and either owned by or leased to, the Insured Organization that are unable to function as intended due to corruption or destruction of software or firmware directly resulting from a Security Breach

FIRST PARTY COVERAGE

Reputation Loss

Loss of income from an Adverse Media Event concerning

- Data Breach,
- Security Breach
- Extortion Threat

Possible Scenarios: Less fees from transit services, parks & rec, Econ Development, etc

FIRST PARTY COVERAGE

Adverse Media Event

Publication by a third party via any medium, including but not limited to television, print, radio, electronic, or digital form of previously non-public information specifically concerning a Data Breach, Security Breach, or Extortion Threat

THIRD PARTY COVERAGE (LIABILITY)

1. Data & Network Liability
2. Regulatory Defense & Penalties
3. Payment Card Liabilities & Costs
4. Website Media Content Liability

THIRD PARTY COVERAGE

Data & Network Liability - aka privacy negligence claims arising from

- Data Breach
- Security Breach
- Failure to timely disclose a Data Breach or Security Breach
- Failure by the Insured to comply with their Privacy Policy that specifically:

(a) prohibits or restricts the disclosure, sharing or selling of PII;
(b) requires providing an individual access to PII or access to correct after a request is made; or
(c) mandates procedures and requirements to prevent the loss of PII;

THIRD PARTY COVERAGE

Privacy Policy

Your public declaration of its policy for collection, use, disclosure, sharing, dissemination and correction or supplementation of, and access to Personally Identifiable Information

THIRD PARTY COVERAGE

Regulatory Defense & Penalties

Legally obligated to pay because of a Regulatory Proceeding first made against any Insured for a

- Data Breach
- Security Breach

THIRD PARTY COVERAGE

Regulatory Proceeding

A request for information, civil investigative demand, or civil proceeding brought by or on behalf of any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity

THIRD PARTY COVERAGE

Regulatory Penalties

- Any monetary civil fine or penalty payable to a governmental entity that was imposed in a Regulatory Proceeding
- Amounts which the Insured is legally obligated to deposit in a fund as equitable relief for the payment of consumer claims due to an adverse judgment or settlement of a Regulatory Proceeding (including such amounts required to be paid into a "Consumer Redress Fund")

Federal, State & Local (Foreign?) – FTC, HHS, FCC, HIPAA, Maryland Agencies, etc

THIRD PARTY COVERAGE

GDPR (EU - General Data Protection Regulation)

Remote possible exposure? Very low & unlikely. However,

- Office of Tourism etc storing EU citizen PII data from targeting ads in EU
- Tracks cookies or IP addresses of EU citizens who visit your website
- Maximum fine of 4% of revenues or 20M Euros ($23M) or
- US allow?

Data & Networking Liability includes:

Non-compliance with the following obligations under the EU General Data Protection Regulation (or legislation in the relevant jurisdiction implementing this Regulation): (a) Article 5.1(f), also known as the Security Principle; (b) Article 32, Security of Processing; (c) Article 33, Communication of a Personal Data Breach to the Supervisory Authority; or (d) Article 34, Communication of a Personal Data Breach to the Data Subject

THIRD PARTY COVERAGE

Payment Card Industry (PCI) Liabilities & Costs

Indemnifies the Insured/Member for PCI Fines, Expenses and Costs which it is legally obligated to pay under a Merchants Service Agreement from a data breach

THIRD PARTY COVERAGE

PCI Fines, Expenses and Costs

Money owed under Merchant Services Agreement as a direct result of a suspected Data Breach.

Includes reasonable and necessary legal costs and expenses incurred to appeal or negotiate an assessment of such monetary amount

THIRD PARTY COVERAGE

Merchants Service Agreement

Any agreement between an Insured and a financial institution, credit/debit card company, credit/debit card processor or independent service operator enabling an Insured to accept credit card, debit card, prepaid card or other payment cards for payments or donations

THIRD PARTY COVERAGE

Website Media Content Liability

Display of Media Material on its web site or on social media web pages created and maintained by or on behalf of the Insured Organization:

1. Defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related to disparagement or harm to the reputation or character of any person or organization
2. A violation of the rights of privacy of an individual, including false light and public disclosure of private facts
3. Invasion or interference with an individual's right of publicity, including commercial appropriation of name, persona, voice or likeness
4. Plagiarism, piracy, misappropriation of ideas under implied contract
5. Infringement of copyright
6. Infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, or slogan, service mark, or service name
7. Improper deep-linking or framing within electronic content

THIRD PARTY COVERAGE

Media Material

Media Material means any information in electronic form, including words, sounds, numbers, images, or graphics and shall include advertising, video, streaming content, web-casting, online forum, bulletin board and chat room content

E-CRIME COVERAGE

- Fraudulent Instruction
- Funds Transfer Fraud
- Telephone Fraud
- Criminal Reward
- Invoice Manipulation
- Cryptojacking

E-CRIME COVERAGE

Fraudulent Instruction

The transfer, payment or delivery of Money or Securities by an Insured as a result of fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions provided by a third party, that is intended to mislead an Insured through the misrepresentation of a material fact which is relied upon in good faith by such Insured.

E-CRIME COVERAGE

Funds Transfer Fraud

The loss of Money or Securities contained in a Transfer Account at a Financial Institution resulting from fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions by a third party issued to a Financial Institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by the Insured Organization at such institution, without the Insured Organization's knowledge or consent.

E-CRIME COVERAGE

Telephone Fraud

The act of a third party gaining access to and using the Insured Organization's telephone system in an unauthorized manner.

E-CRIME COVERAGE

Criminal Reward

Indemnifies the Insured/Member for Criminal Reward Funds for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act

E-CRIME COVERAGE

Invoice Manipulation

Direct Net Loss for inability to collect Payment for any goods, products or services after such goods, products or services have been transferred to a third party, as a result of Invoice Manipulation that the Insured first discovers during the Policy Period.

Invoice Manipulation means the release or distribution of any fraudulent invoice or fraudulent payment instruction to a third party as a direct result of a Security Breach or a Data Breach.

E-CRIME COVERAGE

Cryptojacking

The Unauthorized Access or Use of Computer Systems to mine for Digital Currency that directly results in additional costs incurred by the Insured Organization for electricity, natural gas, oil, or internet.

SERVICE COMPONENT COVERAGE

Beazley services

- Incident Response Planning
- Policies and Procedures
- Risk Assessment
- Training and Online Learning
- Vendor Specialists

https://www.beazleybreachsolutions.com

CYBER SPECIAL OPS, LLC

Cyber Concierge Services

- To provide emergency response to a cyber attack or data breach
- Ransomware Hostage Manual
- 24x7x365 Cyber Emergency Response Team.
- Risk Assessment Tools
- Security Testing
- https://cyberspecialops.com/