Beyond MFA - Proactively Managing Higher Education Cyber Risk In 2023

Gallagher

Insurance | Risk Management | Consulting

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Introductions

Brendan Jaquay – Director | Cyber Liability

Paul Davis – Area Vice President / Regional Director | Cyber Liability

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Agenda - November 3, 2023

I. What are the current cyber risk trends for higher education?

II. What can my institution do to be more resilient to cyber threats and be viewed as a better risk?

III. What are my peers doing to manage cyber risk?

© 2023 ARTHUR J. GALLAGHER & CO.

Cyber Incident Trends in Higher Education

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Trends in Higher Education

Top Patterns

- (36%) System intrusion – lack of patching
- (21%) Miscellaneous errors - misconfiguration
- (19%) Social Engineering – primarily phishing attacks

Data Privacy is a Top Concern

- 497 total Cyber Incidents in this industry
- 48% (238) of incidents had confirmed data disclosure

Threat Actor Motives

- 92% of incidents were financially motivated
- 8% were espionage related from nation-state actors

© 2023 ARTHUR J. GALLAGHER & CO.

2023 Data Breach Investigations Report | Verizon

Connecticut Conference of Independent Colleges (CCIC)

Supply Chain Attacks Impacting Higher Education

MOVEit (2023)

- File transfer application used for the movement of large sets of sensitive data
- Hacker group called CL0P gained access to the application via a zero-day attack
- Affected over 900 higher education institutions breaching millions of PII

Blackbaud (2020)

- Ransomware attack using one of the largest nonprofit technology companies' software
- Millions in sensitive information was encrypted and copied for publishing
- Forensics stopped the encryption of some data but demands were made for copied data

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Ransomware Severity Continues to Rise

Ransomware in Education by the Numbers

	Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
2021	$1,588,468 (median: $558,000)	$196,071 (median: $154,000)	10.5 (median:8)	$68,729 (median: $47,520)	14,168 (median: 1,268)
2022	$1,791,650 (median: $750,000)	$281,525 (median: $175,000)	12 (median: 7)	$68,695 (median: $53,000)	9,567 (median: 415)

BakerHostetler_Data_Security_Incident_Response_Report_(bakerlaw.com)

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Emerging Cyber Risk - Tracking Technologies

WHAT IS WEB TRACKING TECHNOLOGY AND WHY IS IT RISKY?

- **What:** Web tracking technologies collect information about users as they interact with websites or mobile applications (e.g., cookies, web beacons, Google Analytics)
- **Why**: Organizations that know how users are interacting with their websites can enhance user experience or better target digital marketing and advertising
- **Who**: The technology can be developed internally or obtained from third parties that want to monetize the information

THE CURRENT LEGAL LANDSCAPE

- Scores of ***class action lawsuits*** have been filed alleging privacy violations due to web tracking – and more are expected
- ***Regulators at all levels are becoming increasingly assertive*** about requiring processes and safeguards in the use of we tracking technologies on individuals
- Has lead to ***substantial costs*** in responding to lawsuits, regulatory investigations, fines and settlements

MITIGATING DATA TRACKING LIABILITIES

- ***Coordination is key*** among marketing, legal and risk management teams
- ***Review contracts*** with vendors and other third parties that use the data you collect
- ***Understand the restrictions and obligations*** imposed by the various laws (e.g., HIPAA, VPPA, wiretapping statutes) that regulate collection and use
- ***Engage with privacy experts*** to address your legal obligations regarding notice, consent and use in connection with the collection of user data

INSURANCE COVERAGE

- ***Cyber insurers are becoming increasingly cautious*** about covering liabilities arising from web tracking claims – especially from class action lawsuits
- Insureds may be subject to ***sub limits, coinsurance, partial coverage, or even outright exclusions*** for this exposure
- ***Exclusions*** may not be clearly stated but instead contained in subtle language that does not obviously apply to this exposure

- Speak to campus communications / marketing / vendors about use
- Perform an analysis of VPPA, BIPA, GIPA, California's wiretapping law and HIPAA, FERPA compliance
- Update Privacy Policy
- Evaluate costs/benefits

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Artificial Intelligence Use and Risks Increase

WSJ PRO

ChatGPT Helped Win a Hackathon

A team from cybersecurity firm Claroty used the AI bot to write code to exploit vulnerabilities in industrial systems

Two security researchers from cybersecurity company Claroty Ltd. said ChatGPT helped them win the Zero Day Initiative's hack-a-thon in Miami last month.

Generative AI Could Revolutionize Email—for Hackers

Phishing attempts can already be made indistinguishable from legitimate emails, with all red flags eliminated. But some security experts are using the technology to get ahead of attackers

By James Rundle

Sept. 6, 2023 5:30 am ET | WSJ PRO

Biden Issues Executive Order to Create A.I. Safeguards

The sweeping order is a first step as the Biden administration seeks to put guardrails on a global technology that offers great promise but also carries significant dangers.

intelligence on Monday, requiring that companies report to the federal government about the risks that their systems could aid countries or terrorists to make weapons of mass destruction. The

Bloomberg

Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

- Develop an acceptable use policy
- What should it include?

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Fear of cyber warfare and critical infrastructure failure

- Ukraine | Russia
- Hamas | Israel
- China
- Iran
- North Korea

- Intellectual property theft
- Widespread impact
- Insurability

© 2023 ARTHUR J. GALLAGHER & CO.

Critical Information Security Controls

from the perspective of a cyber risk management professional

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Identity Access Management | Advanced Multi-factor Authentication

Authentication tool ensuring a user is who he or she claims to be

- Three main types
  1. Something you know (e.g. PIN or password)
  2. Something you have (e.g. token or smart card)
  3. Something you are or do (e.g. biometrics or fingerprint)
- Best in class – FIDO (Fast Identity Online)
  - Provides public-key cryptography – device creates a pair of keys -> one kept on local device and the other stored in online service
  - Requires either a biometric check on a smart device or a hardware token for access to be granted
  - Contextual, hardware/application based | not SMS / phone call

MFA in front of:
- Faculty / Staff Email
- Remote Access (i.e., RDP & VPN)
- Privileged Access
- Critical Software as a Service (SaaS) Applications
- Data Backups

Endpoint Protection

Security solutions that continuously monitor end-user devices, servers and cloud assets to detect and respond to suspicious activity, including malware

- Key functions:
  - Discover anomalous activity – applies behavioral analytics to detect any suspicious behavior
  - Real-time visibility into the endpoint – comprehensive look into everything happening on your network's endpoints
  - Fast and decisive remediation – Top EDR solutions can isolate the endpoint through automation for threat containment allowing organizations to take action quickly
- Best in class – CrowdStrike Falcon, Sentinel One ; 100% deployment ; Managed solution preferred

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

MFA Prompt-bombing Attack

Data Leak Occurs

- User credentials (username, password, recovery information) are leaked
- Leaked credentials may be sourced from a preliminary attack from phishing or social engineering
- Leaked credentials could also have been from a larger breach that was released to the dark web

Stolen Credentials are Used

- Threat actor then attempts to use the illicitly gained credentials to sign into the account
- User's account is secured by push multi-factor authentication and prompts user to authenticate
- Prompts can occur via email, desktop notification, text message, but most frequently occur through mobile notification

Victim receives notification and "fatigue" occurs

- Victim receives numerous push notifications happening in rapid intervals
- In efforts to stop the notifications, victims select "yes" in hopes to stop receiving alerts
- Threat actor can sometimes contact victim claiming maintenance procedure
- Threat actor authenticates and ultimately authorizes entry

Threat Actor Causes Havoc on Network

- Personally Identifiable Information (PII) is accessed and exfiltrated while critical networks are shut down while a ransom is demanded
- Insureds may be subject to ***sub limits, coinsurance, partial coverage, or even outright exclusions*** for this exposure
- ***Exclusions*** may not be clearly stated but instead contained in subtle language that does not obviously apply to this exposure

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Patching, Vulnerability Management & Attack Service Monitoring

Formalized process for acquiring, developing, maintaining and disposing of all assets on your network

- Asset inventory should include the asset owner, location, cost, value (classification), duration, and any dependencies
- Tools should be able to include all of the above, as well as the ability to deploy patches to software as needed
- Best in class – Tools like SysAid among others
  - Asset management for all devices on your network through a dashboard
  - Patching and operating system updates can be deployed automatically to individual or multiple endpoints remotely
- Acknowledgment of the challenges of monitoring a cloud, multi-cloud, on premises, micro-application integrated digital environment
  - Hearing more conversations about the need for tools that automate data & asset discovery, create and update asset/data inventories, and cloud security configuration checks
- Continuous vulnerability scanning and automated patching is no longer enough because underwriters acknowledge that you need to know what's in your environment and where's it's located in order to scan/remediate/enforce policies

Robust Backup Procedures

The process of creating and storing copies of data that can be used to protect organizations from business interruption

- Backups can be full (most lengthy), differential, and incremental (fastest method)
- Should be stored in multiple locations (onsite/offsite), cloud, hot/warm/cold sites
- Best in class method – 3-2-1 method
  - 3 copies of data
  - Two kept locally, one stored offsite (including cloud)

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Security Awareness and Phishing Training

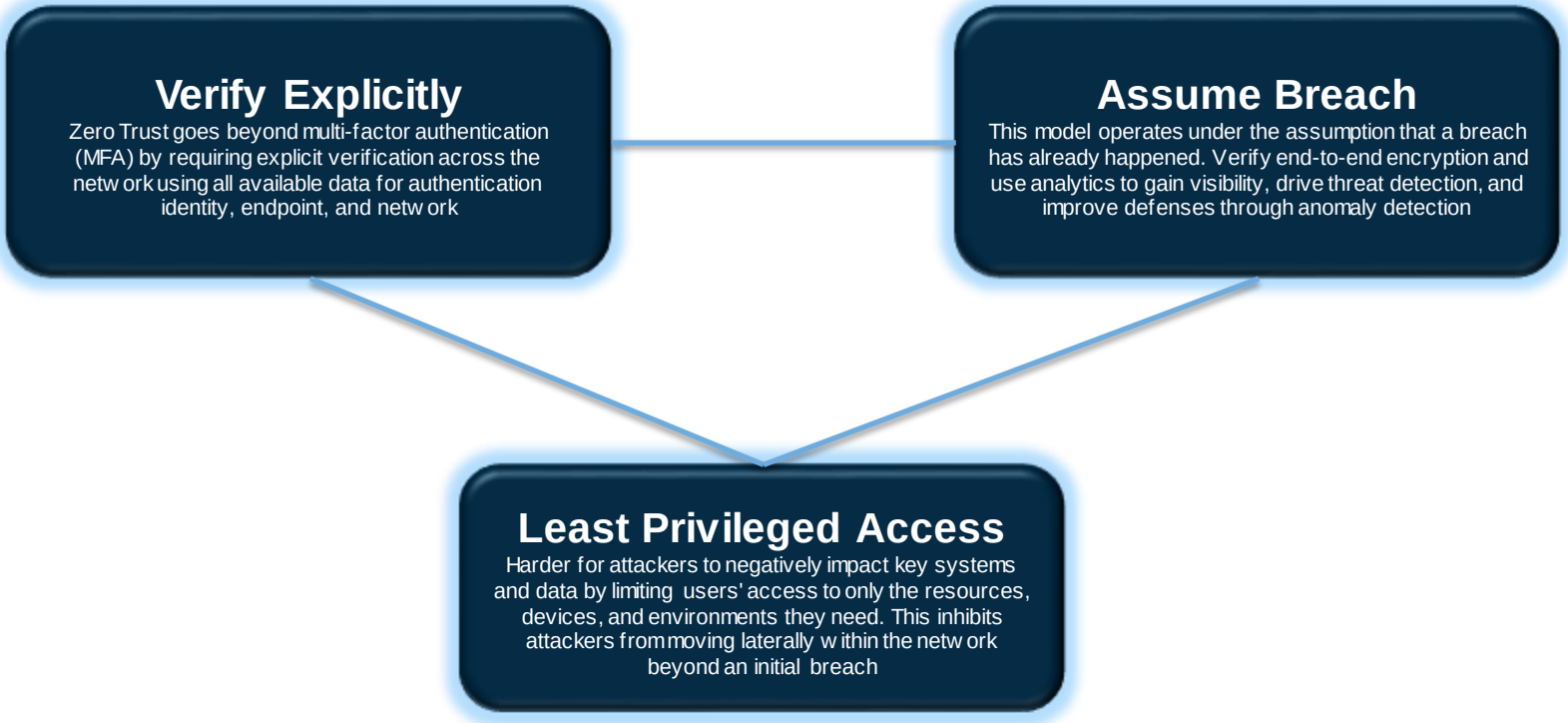
Strategic approach taken to educate and train all employees, contractors and stakeholders on the importance of cybersecurity and data privacy

- Objective – enhance security awareness among employees while reducing cyber risk from human error
- Phishing – has become highly sophisticated with the help of artificial intelligence
  - Cannot be prevented purely through technical means
  - Training educates employees on how to spot and report suspected phishing attempts via email, phone or text message
    - Track click rates and reporting rates to better track company resiliency
    - Increase training for employees with higher click rates
- Security Training can be provided through online videos (most common), company/department meetings, written documents, classroom training or a combination
- Key components for effective training – successful launch, management (any employee) buy-in, office reminders (e.g. posters)
- Best in class
  - Quarterly phishing campaigns against all users, including students
  - Re-train repeat Faculty/Staff clickers

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Leveraging a Zero Trust model with three principles



© 2023 ARTHUR J. GALLAGHER & CO.

How are your higher education peers addressing cyber risk?

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Ways to mitigate cyber risk

- Improve INFOSEC controls through technology and people
- Partner with respected IT and INFOSEC vendors – prior to an incident
- Seek and share best practices (i.e., MS-ISAC, NIST, CISA, FBI, DoED, CCIC, Peers…)
- Coordinate & Educate Administration, Faculty, Risk Management, Campus Security, IT, IT Security, Business Officers, Legal, Privacy, Compliance, Communications around this important shared institutional issue
- Strengthen vendor contracts
- Develop plans and practice cyber incident response
- Consider risk transfer through cyber insurance

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Incident Response Plans & Table Top Exercises

- Written plans that outline key stakeholders and immediate triage group
- Outline channels of communication
- Playbooks for specific cyber loss scenarios
- Tested at least annually with real life scenarios
- “Living” document
- Solicit input from trusted third parties
- Cyber insurance carriers may offer complimentary or discounted table top exercises with experts

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

Risk Transfer – What are your peers buying in cyber insurance limit?

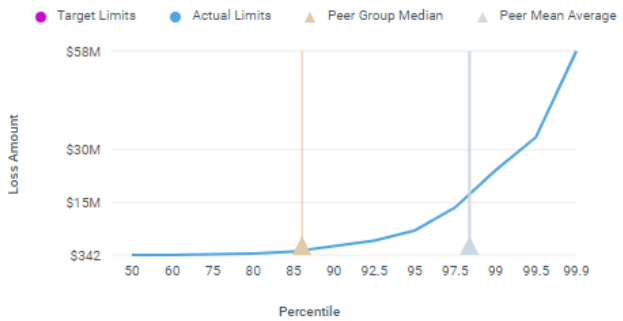
Peer Group Average	98th	Your peer group (mean) average limits is transferring financial risk for 98% of simulated cyber losses.
	$17.1M	Your equivalent limits at this peer percentile
Peer Group Median	86th	The peer median company is transferring financial risk for 86% of simulated cyber losses.
	$1.3M	Your equivalent limits at this peer percentile

CONNECTICUT COLLEGE

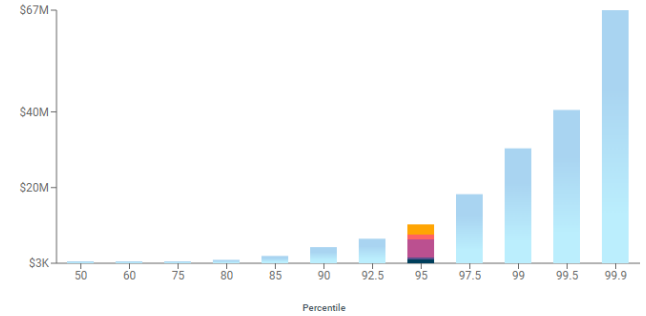
Peer Group Average Comparison (for Aggregate Severity Distribution)

PEER GROUP INFO

Education | Small: (10M–250M) | more than 100 Peers



Software Impairment Loss Contributions



95th Percentile

$10,271,000

Investigation & Response	$2,641,000
Digital Assets / Data Restoration	$1,248,000
(Contingent) Business Interruption	$4,760,000
Regulatory Costs	$510,000
Legal Liability	$1,111,000

* The loss contribution values may not add up due to rounding.

© 2023 ARTHUR J. GALLAGHER & CO.

Connecticut Conference of Independent Colleges (CCIC)

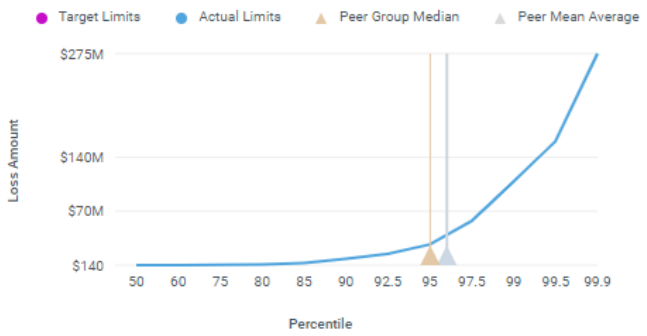
Risk Transfer – What are your peers buying in cyber insurance limit?

Peer Group Average	96th	Your peer group (mean) average limits is transferring financial risk for 96% of simulated cyber losses.
	$39M	Your equivalent limits at this peer percentile
Peer Group Median	95th	The peer median company is transferring financial risk for 95% of simulated cyber losses.
	$26.8M	Your equivalent limits at this peer percentile

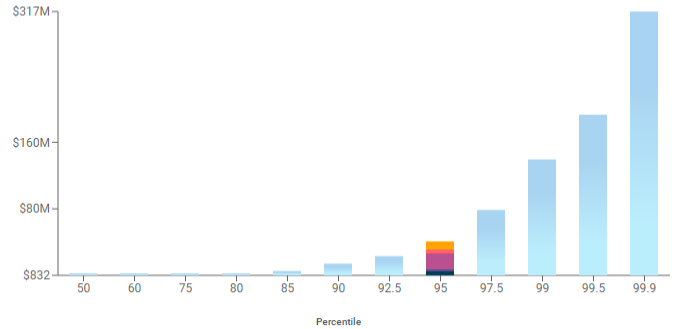
Yale

PEER GROUP INFO

Education | Large: (1B+) | less than 10 Peers



Software Impairment Loss Contributions



95th Percentile

$40,815,000

Investigation & Response	$10,080,000
Digital Assets / Data Restoration	$4,715,000
(Contingent) Business Interruption	$19,028,000
Regulatory Costs	$1,911,000
Legal Liability	$5,081,000

* The loss contribution values may not add up due to rounding.

© 2023 ARTHUR J. GALLAGHER & CO.

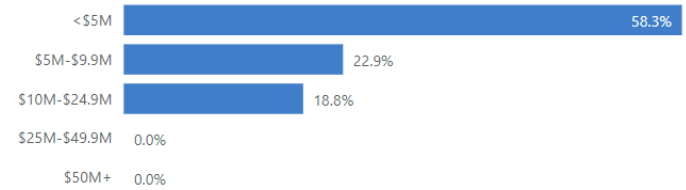
Connecticut Conference of Independent Colleges (CCIC)

Risk Transfer – What are your peers buying in cyber insurance limit?

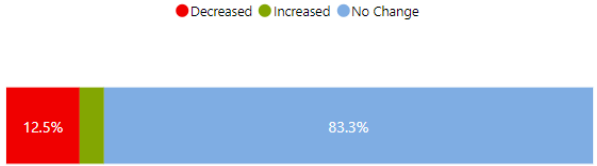
2022 Liability Benchmark Report - 4-year private

Peer Count	Selected Region	Selected Enrollment	Selected Endowment	Selected Operating Budget
57	Northeast	All	All	All

Range of Cyber Liability Limits

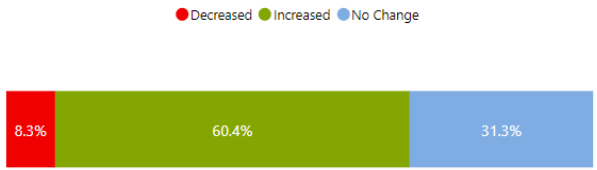


Changes in Cyber Liability Limit in Last Two Years

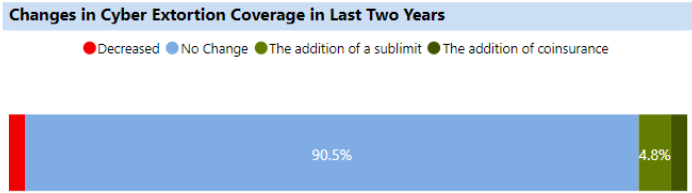


Range of Cyber Liability SIR

Changes in Cyber Liability SIR in Last Two Years



Changes in Cyber Extortion Coverage in Last Two Years



© 2023 ARTHUR J. GALLAGHER & CO.

Thank You! **Questions?**

Paul B Davis
Vice President & Regional Director, US Cyber Practice
Paul_Davis1@ajg.com
303.250.6156

Brendan Jaquay
Director, Cyber Practice
Brendan_Jaquay@ajg.com
215.390.0550

The information contained herein is offered as insurance Industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Insurance brokerage and related services provided by Arthur J. Gallagher Risk Management Services, LLC. (License Nos. 100292093 and/or 0D69293).

Gallagher

Insurance | Risk Management | Consulting

© 2023 ARTHUR J. GALLAGHER & CO.