Cyber Insurance with Aon Risk Solutions

National CyberWatch Center
Prince George’s Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org
Webinar Protocol

:: Mute your phone/mic when not talking

:: Questions during the webinar? Use Chat feature

:: Technical problems:

info@nationalcyberwatch.org
About the 2016 Webinar Series (con’t)

:: Great topics

:: Recorder & archived on National CyberWatch Center YouTube channel:

https://www.youtube.com/user/CyberWATCHcenter
About the 2016 Webinar Series (con’t)

:: Sign up for future webinars here:

http://www.nationalcyberwatch.org/programs-resources/webinar-series
Moderator

:: Casey W. O’Brien
:: Executive Director, National CyberWatch Center
:: cobrien@nationalcyberwatch.org
Panelist

:: Andrew Laubmeier
:: Broker
:: Aon Risk Solutions
:: Financial Services Group
Cyber Insurance Overview
Aon’s Professional Risk Solutions Team – Fast Facts

50+ Global Dedicated Aon Professionals
US / London / Bermuda

Industry Specialist Brokers align with Aon Industry Practices

200+ Cyber Claims Handled Since 2012

$400+ Million Premium Placed (2015)

1,500+ PRS Clients
What is Cyber Liability Insurance?
Scope of Growing & Emerging Threats

- Vendors
- Cloud
- Media
- Security & Privacy
- Continuity
- Contracts
- Trademark
- Defamation
- Copyright
- Patent
- BYOD
- Unlawful Collection
- BYOC
- Geo-location
- Business Interruption
- Reputation
- Social
- Regulatory
- Insurance
- International
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
- Unlawful Collection
- Breach of Contract
- Incident Response
- Digital Migration
- Payments
- Mobile
- Big Data
- Technology
Just for hackers, right?
What is Cyber?

Where
- Online
- Offline

Who
- Malicious
- Accidental
- Internal
- External

What
- Technology
- Media
- Protected Data

Financial Impact
- Crisis Expense
- Extra Expense
- Lost Income
- Defence Expense
- Regulatory Fine
- Liability
Overview of Insuring Agreements
Overview of Available Coverages

THIRD PARTY LIABILITY (triggered by a claim)

- **Security Liability:** Coverage for defense costs and damages the insured is legally obligated to pay resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, and unauthorized use, denial of service attack or transmission of a computer virus.

- **Privacy Liability:** Coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential corporate information, whether or not due to a failure of network security. Includes unintentional violations of your privacy policy and misappropriation that results in identity theft.

- **Privacy Regulatory Proceedings (usually sub-limited):** Coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information. Insuring agreement may include (depending on insurer) coverage for fines and penalties to the extent insurable by law. Coverage for damages, i.e. amounts the insured is required by settlement to deposit into a consumer redress fund, may be covered depending on the insurer.
Overview of Available Coverages

THIRD PARTY LIABILITY (triggered by a claim)

- **Media Liability**: Coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright, title trademark infringement, or invasion of privacy with respect to creation and dissemination of your content on your website including advertising.

- **Payment Card Industry Data Security Standards (PCI-DSS)**: Coverage for a contractual fine or penalty (monetary assessment if available) from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an “Acquiring Bank”) in connection with an Insured’s non-compliance with PCI Data Security Standards.

- **Cyber Extortion**: Reimburses the insured for expenses incurred in the investigation of an intentional computer attack or threat against the insured and any extortion payments made to prevent or resolve the threat. Payments are generally subject to full discretion by insurer.
Overview of Available Coverages

FIRST PARTY COVERAGE (triggered by discovery of an incident)

- **Privacy Event Expenses (usually sub-limited):** Coverage for your fees and expenses due to a potential or actual violation of a privacy regulation. Covered expenses can include computer forensics expenses, costs for a public relations firm and related advertising to restore your reputation, notification expenses and credit monitoring services.
  - IT forensics expenses
  - Legal expenses
  - Notification to consumers
  - Consumer credit monitoring services
  - Public relations expenses to restore insured’s reputation

- **Network Business Interruption:** Reimburses the insured for actual lost net income and extra expense incurred when the insured’s computer system is interrupted or suspended due to a failure of network security. Dependent Business Interruption is also available, but often subject to a sub-limit. Additionally, System Failure coverage is available upon request which provides limited coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security. In addition to a dollar amount retention, a waiting period retention of between 10 to 24 hours applies.

- **Digital Asset Protection:** Reimburses the insured for costs incurred to restore or recreate intangible, non-physical assets (software or data, including electronically stored credit card numbers and customer databases) that are corrupted, destroyed or deleted due to a network security attack.
### Scope of Cyber Insurance Coverage

#### Defense Costs + Damages + Regulator Fines

#### Liability Sections
- Failure of Network Security
- Failure to Protect/ Wrongful Disclosure of Information, including employee information
- Privacy or Security related regulator investigation
- All of the above when committed by an outsourcer
- Wrongful Collection of Information (some policies)
- Media content infringement/ defamatory content

#### First Party Sections
- Network-related Business Interruption
- Extra Expense
- System Failure Business Interruption (some policies)
- Dependent Business Interruption (some policies)
- Intangible Asset damage

#### Expenses Paid to Vendors
- Crisis Management
- Breach-related Legal Advice
- Call Center
- Credit Monitoring, Identity Monitoring, ID Theft Insurance
- Cyber Extortion Payments

#### Insured’s Loss
- Extra Expense
  - System Failure Business Interruption (some policies)
  - Dependent Business Interruption (some policies)
  - Intangible Asset damage
Cyber Statistics
Claims by Revenue Size

- Smaller organizations experienced the most incidents – those with revenues <$2B made up 57.9% of the incidents
- While Mega-Cap companies accounted for only 1.4% of claim events, they were responsible for 45.6% of records exposed
- “Unknown” represents companies where revenue size was not reported during the course of the study

Source: NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims: A Study of Actual Claims Payouts
Root Causes of a Data Breach

Distribution of root cause of data breach

- Malicious or Criminal Attack: 49%
- System Glitch: 32%
- Human Error: 19%

Per capita cost for root causes of the data breach

- Malicious or Criminal Attack: $230
- System Glitch: $210
- Human Error: $198

Source: Ponemon Institute 2015 Cost of Data Breach Study
Potential Elements of Coverage in Commercial Property, General Liability, Crime, and Kidnap & Ransom Policies

**Property Insurance:**
Malware and Denial-of-Service attacks do not constitute ‘physical perils’ and do not damage ‘tangible property’

**Errors and Omissions:**
- Unauthorized access exclusions.
- Requires negligence in provision of defined business activities.

**Common Hurdles:**
- No coverage for expensive crisis expenses required by law or to protect reputation.

**General Liability Insurance**
CGL Privacy coverage limited to ‘publication or utterance’ resulting in one of traditional privacy torts.

**Crime Coverage**
Crime policies require intent… theft of money, securities, or tangible property.

Can’t ‘Traditional’ Insurance Help?
Types of Data Breaches in Higher Education

- 36% Hack or Malware
- 30% Unintended Disclosure
- 17% Portable Device
- 7% Stationary Device
- 5% Physical Loss
- 1% Insider
- 3% Payment Card Fraud
- 1% Unknown

Source: Educause
2015 URMIA Cyber Survey

URMIA surveyed its members in March 2015 to find out what the current practices are for purchasing Cyber Liability Insurance (Cyber) in higher education. The goal of this survey was to provide the URMIA membership with an understanding of:

From the 109 survey responses, the key findings of the survey are:

1. About 68 percent of respondents purchase Cyber; about 70 percent having done so within the last three years. Those who do not purchase Cyber are re-evaluating their decision.
2. Respondents from private institutions purchase Cyber more often than those from publics while smaller institutions purchase Cyber more often than larger ones. Private institution purchase higher limits than publics as do larger institutions than smaller.
3. Most institutions that purchase Cyber have limits of $5 million or less and deductibles of $50,000 or less.
4. In their purchasing decisions, institutions value insurer coverage of the cost of data breach notification and credit monitoring and assistance with complying with notification laws for multiple jurisdictions.
5. Nearly a third of the respondents have filed a claim under their Cyber and have been satisfied with the insurers response.
Examples
## Higher Education – Claims Response

<table>
<thead>
<tr>
<th>Claims Example</th>
<th>Would a Cyber Policy Respond?</th>
<th>Insuring Agreement Triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Penn State – 18,000 records compromised – 5/15/2015</strong></td>
<td><strong>YES</strong></td>
<td><strong>First Party Breach Response, Including:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Forensics Investigation to determine what and how records were compromised</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Legal Expense to determine if legal obligation to notify exists, and advise on information to include within notice letters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Costs to notify individuals, including credit monitoring, ID protection, and call center services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Crisis Management to respond to breaches, including PR expenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Third Party Claims– Network Security &amp; Privacy</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Class actions for financial Damages, personal injury</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Regulatory Fines &amp; Penalties</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- In the event regulatory bodies decide to investigate the breach, coverage would include defense, fines and penalties assessed where insurable by law</td>
</tr>
</tbody>
</table>

Penn State’s College of Engineering announced in May 2015 that their servers were hacked in two different intrusions. The hackers are believed to be based in China and may have exposed “at least 18,000 people and possibly other sensitive data”.

Penn State’s President sent a letter out to students and faculty informing them that the college’s network had been disconnected to the Internet while they investigate the intrusion. All College of Engineering faculty, staff and students were affected.
# Higher Education – Claims Response

<table>
<thead>
<tr>
<th>Claims Example</th>
<th>Would a Cyber Policy Respond?</th>
<th>Insuring Agreement Triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Riverside Community College – 35,212 records compromised – 5/30/2014</td>
<td>YES</td>
<td>First Party Breach Response, Including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Forensics Investigation to determine what and how records were compromised</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Legal Expense to determine if legal obligation to notify exists, and advise on information to include within notice letters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Costs to notify individuals, including credit monitoring, ID protection, and call center services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Crisis Management to respond to breaches, including PR expenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third Party Claims – Network Security &amp; Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Class actions for financial Damages, personal injury</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regulatory Fines &amp; Penalties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- In the event regulatory bodies decide to investigate the breach, coverage would include defense, fines and penalties assessed where insurable by law</td>
</tr>
</tbody>
</table>

Riverside Community College suffered a data breach affecting 35,212 students in May 2014 when a district employee emailed a file containing information about all students who were enrolled in the spring term to a colleague working at home due to illness, for a research report that was on a deadline. The district employee used a personal email account to send the data because the file was too large for the district’s secure email to send. The employee then typed in the incorrect email address.

The information contained in the file included names, addresses, birth dates, Social Security numbers, email addresses, student ID numbers, and telephone numbers.
## Higher Education – Claims Response

<table>
<thead>
<tr>
<th>Claims Example</th>
<th>Would a Cyber Policy Respond?</th>
<th>Insuring Agreement Triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Johns Hopkins – 1,307 records compromised – 3/7/2014</td>
<td>YES</td>
<td>First Party Breach Response, Including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Forensics Investigation to determine what and how records were compromised</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Legal Expense to determine if legal obligation to notify exists, and advise on information to include within notice letters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Costs to notify individuals, including credit monitoring, ID protection, and call center services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Crisis Management to respond to breaches, including PR expenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third Party Claims– Network Security &amp; Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Class actions for financial Damages, personal injury</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Extortion –</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Any threats to compromise information unless the hacker is paid a monetary demand</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regulatory Fines &amp; Penalties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- In the event regulatory bodies decide to investigate the breach, coverage would include defense, fines and penalties assessed where insurable by law</td>
</tr>
</tbody>
</table>

“University officials at Johns Hopkins University announced a data breach of their Department of Biomedical Engineering’s Design Team course web server. A hacker claiming to be part of the group Anonymous claimed credit for the hack.”

The hackers made an attempt to extort the university out of server passwords, but the university did not comply with the request. Those affected include any students from the BME department who were enrolled in the course from 2006 to this past fall. Approximately 1,307 individuals may have been affected.

Although the breach happened late last year, it was not realized until someone posted on Twitter in January that the server was open to attack.
Questions?
Next Webinar: April 28, 2016

:: April 28
:: 2-3pm ET
:: Threat Intelligence with Threat.Connect
Thanks!

:: Check your inbox for future webinar invitations and links to today’s recording
:: Past Webinars on NCC website
:: National CyberWatch YouTube Channel