Leveraging Best Practices to Determine your Cyber Insurance Needs

Sector Conference, Toronto
November 2017
Chubb Disclaimer

The views, information and content expressed herein are those of the author and do not necessarily represent the views of any of the insurers of The Chubb Group of Insurance Companies. Chubb did not participate in and takes no position on the nature, quality or accuracy of such content. The information provided should not be relied on as legal advice or a definitive statement of the law in any jurisdiction. For such advice, an applicant, insured, listener or reader should consult their own legal counsel.
Presenters:

Matthew Davies, Vice President
Canadian Product Manager – Professional, Media & Cyber Liability
Chubb Financial Lines

Dave Millier, CEO
UZADO
Agenda

• Cyber Insurance 101
  – Cyber Exposures – beyond just IT issue
  – What does a Cyber Policy cover?
  – Cyber Claims – What Have We Been Seeing?
  – Cyber Underwriting Process
• Cyber COPE®
• From Concept to Reality
• Sample Cyber COPE® Score Card
• Summary
Cyber Insurance 101
What the Privacy Commissioner of Canada Wants to Know

Be prepared to respond to at least the following four questions during a privacy regulatory investigation of a security incident in your organization:

- Show us your organization’s information security governance program.
- Show us evidence of regular training and awareness.
- Show us evidence of your compliance monitoring.
- Show us your organization’s security incident protocol, and walk us through how you implemented it.

No matter how good your Security Controls are...

"I TOLD YOU SOMEONE WAS PHISHING AND NOT TO OPEN THAT ATTACHMENT!"
Cyber insurance in a nutshell

Incident Response
- Coach Services
- Legal Services
- Forensics
- Notification
- Credit Monitoring
- Public Relations

First-Party
- Extortion
- Business Interruption
- Restoration
- Cyber Crime

Third-Party
- Privacy Liability
- Network Liability
- Media Liability
- Technology E&O

+ Regulatory Defence
+ PCI Assessment
Chubb Exposure Stats by Trigger Over the Last Decade

- **Lost/Stolen Devices**
  - 2014 – 14%
  - 2015 – 11%
  - 2016 – 10%
  - 2017 – 6%

- **Hack**
  - 2014 – 27%
  - 2015 – 40%
  - 2016 – 33%
  - 2017 – 20%

- **Rogue Employee**
  - 2014 – 15%
  - 2015 – 13%
  - 2016 – 5%
  - 2017 – 15%

Source: Chubb’s claims data as of October 2017 – based on approximately 3,000 Claims.
Chubb Cyber Bad Actors Over the Last Decade

- **Internal**
  - Employees, independent contractors, interns

- **External**
  - Criminal groups, hackers, former employees, government entities

- **Partner**
  - Suppliers, vendors, outsourced IT, hosting providers

*Source: Chubb’s claims data as of October 2017 – based on approximately 3,000 Claims.*
Chubb Cyber Affected Assets Over the Last Decade

**Server**
- Database, email, virtual, physical, web

**Network**
- Local, wireless, routers, firewalls

**User Device**
- Desktop, laptop, smartphone, POS terminal

**Public Terminal**
- ATM machines, pay at pump gas stations

**Media**
- Paper documents, USB drives, CDs

**People**
- Developer, admin, executive, end user

*Source: Chubb’s claims data as of October 2017 – based on approximately 3,000 Claims.*
Cyber Targets by Organization’s Employee Count

**2011**

- Large 2,500+: 50%
- Medium 251 to 2,500: 32%
- Small 1 to 250: 18%

**2016**

- Large 2,500+: 35%
- Medium 251 to 2,500: 34%
- Small 1 to 250: 31%

Source: Symantec Internet Security Threat Report 2017 Volume 22
The “Perfect” Risk

What Underwriters are looking for:

– Board level and executive management engagement
– Enterprise wide risk management attitude
– Up-to-date data security and privacy policies
– Annual employee awareness training
– Incident management plans (BCP, DRP, IRP)
– Data protections – encryption, segregation, back-ups, device tracking
– Vendor due diligence
– Continuous improvement

“OFFHAND, I’D SAY WE HAVE AN ACCOUNTABILITY PROBLEM!”
Cyber COPE®
Pop Quiz

Part 1 – Property Assessment
1. How many floors are in your office building?
2. Can you name three materials that your office building is made of?
3. Does your building have a central fire detection alarm system?

Part 2 – Cyber Assessment
1. Does your company encrypt all sensitive data at-rest and in-transit?
2. Do you provide your staff with training on systems security?
3. Does your company use any unsupported software?
Question

So if the number of floors in a building or the age of a sprinkler system can be used to help assess your commercial property risk, why can’t something like the number of computers or the currency of software in service in a company be used to more accurately assess cyber risk?
COPE Property Underwriting Framework

- Occupancy
- Protection
- Construction
- Exposures
What makes COPE effective for property?

- It’s simple to understand
- Provides objective data points
- Provides subjective data points
- Balance of objectivity and subjectivity
- Use of publicly available information
- Promotes discussions on loss control
Cyber COPE®

Launched in 2016, a new model for cyber underwriting, intended to simplify and improve the assessment of both cyber and privacy risks with four primary goals:

1. Accessible to both technical and non-technical audiences
2. Provide both objective and subjective measurements
3. Foster information sharing so that organizations can learn from each other to help mitigate future losses
4. Open opportunities for innovation by the insurance and security industry
Cyber COPE® Proposed Cyber Risk Underwriting Framework

- Organization
- Protection
- Components
- Exposures

Cyber COPE®
## Transforming COPE to Cyber COPE®

<table>
<thead>
<tr>
<th>COPE</th>
<th>Cyber COPE®</th>
<th>Measurement</th>
<th>Sample Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Construction</td>
<td>Components</td>
<td>Objective</td>
<td>Number of endpoints and network connections, software versions, and data center locations</td>
</tr>
<tr>
<td>Occupancy</td>
<td>Organization</td>
<td>Objective</td>
<td>Policyholder’s industry, quality of IT and security related policies, and use of industry standards, revenue, IT security budget, compliance (PCI DSS, other standards)</td>
</tr>
<tr>
<td>Protection</td>
<td>Protection</td>
<td>Subjective</td>
<td>Data retention policies, firewalls, monitoring, and incident response/response readiness policies</td>
</tr>
<tr>
<td>Exposures</td>
<td>Exposures</td>
<td>Subjective</td>
<td>Political or criminal motivation, types of outsourcing, and type/amount of sensitive information</td>
</tr>
</tbody>
</table>
Cyber COPE® Usage

• **Current**
  – Full cyber white paper published on Chubb.com
  – Assessment to support Chubb’s Global Cyber Facility
  – FireEye’s Cyber Insurance Risk Assessment (CIRA)

• **In Progress**
  – Adapt underwriting questionnaire for use with Small Commercial and Middle Sized Enterprise Customers
  – Alignment with other industry standards ISO27001, NIST, PCI-DSS, OCE
  – Integration with internal data analytics and external partners
INSURANCE TO PROTECT SOMETHING YOU CAN’T TOUCH FROM PEOPLE YOU CAN’T SEE... THE WORLD IS GETTING STRANGER STILL.
A Brief History – Uzado and Cyber COPE®

• Russ Cohen publishes a white paper Cyber COPE® – Transforming Cyber Underwriting

• Uzado and Russ chat and discuss cyber risk and how insurance can play a pivotal role

• Uzado proposes to build the initial draft framework leveraging industry best practices, the NIST Cybersecurity Framework (CSF) and the Center for Internet Security Critical Security Controls (CSC)

• Uzado builds the draft framework into a working model including risk measures, maps the framework against other industry frameworks and standards

• Uzado and Chubb look for opportunities to leverage the framework in existing insurance practices
Cyber Security Lifecycle
Aligning the Lifecycle to Maturity Levels

• Lifecycle broken into 4 phases, each feeds the next phase

• Companies need to determine where they are at in the lifecycle as it relates to their cyber risk maturity level

• Each level of the lifecycle corresponds to a maturity level
  – Planning = Maturity Level 1 Company is just starting out on their cybersecurity journey
  – Implementation = Maturity Level 2 Company has identified what they need to do to improve their risk posture and has started to take steps forward
  – Manage = Maturity Level 3 Company has implemented various security safeguards and is actively managing them with a goal of identifying security threats and responding in real-time
  – Validate = Maturity Level 4 Company is periodically testing their security controls for effectiveness, performing continuous improvement activities, restarting the lifecycle as appropriate
Aligning The Lifecycle to Cyber COPE®

**Plan:**
- Determine what Components make up the network
- Identify the maturity level of the Organization
- Decide what Protections are required
- Capture an accurate list of any Exposures the Organization may face

**Implement:**
- Build out any policies and processes that are required
- Deploy tools and technologies to better secure the environment
- Ensure that any identified exposures have at least one corresponding protection

**Manage:**
- Ensure policies and processes are mapped to workflow activities that will help you not just
- Attain some level of risk management but also maintain it on an ongoing basis

**Validate:**
- Build and follow a set of activities that help to measure the effectiveness of each control
- Rinse and repeat as often as deemed necessary
Standards and Frameworks and Best Practices, Oh My!

• Logical next step was to map the Cyber COPE® controls to various other controls
• To date, we have mapped:
  – NIST CSF
  – CIS CSC
  – OSFI CSA
  – NERC CIP
  – PCI

Goal is to allow organizations to gain insights into where they are currently at as it relates to various other standards, frameworks, or best practice activities
Using Cyber COPE ® to Determine Risk

• Score is mapped to other frameworks and uses a maturity model that looks something like:
  • 1 = Ad Hoc or not doing it
  • 2 = Partially Implemented
  • 3 = Mostly Implemented
  • 4 = Implemented, Continuous Improvement
  • N/A = Not Applicable

• Based on the answers to the Cyber COPE ® questions, along with the self ranking of maturity, determine an initial Risk Score

• Compare the Score against other companies in the same industry

• Provide guidance and recommendations on remediation activities based on areas that are ranked lower and require further attention

• Assume anything lower than 3 should be addressed
Cyber COPE® to Determine Appropriate Insurance Products

• Some of the Cyber COPE® questions focus on certain areas that insurance would be appropriate to protect

• For example, a company that has a lot of credit card data may want to purchase additional insurance that would provide identify theft monitoring to clients affected by a breach

• A company that relies on a third party’s IP (Intellectual Property) may purchase insurance that protects it in the event the IP entrusted to that organization by its business partners is stolen, tampered with, or deleted

• A company that relies heavily on the Internet to deliver services may buy business interruption insurance to protect them in the event they are subjected to a DoS (Denial of Service) which impacts them to the point where they cannot deliver services to their clients
Gaining Traction for Cyber COPE® – It Takes Time

- The Cyber COPE® framework will take time to be adopted

- Needs industry recognition, review and validation

- Insurance companies will need to get used to seeing the Cyber COPE® results as part of cybersecurity insurance application documents

- Start out with a small set of questions, get companies comfortable, then present the more comprehensive questionnaire

- Use it as part of an overall insurance quotation and coverage, not just for cyber insurance
Measure A Little, Then a Lot

• Ask a few questions to introduce the concept of Cybersecurity risk

• Based on answers, present findings in a non-technical, easy to understand answer complete with explanations and recommendations

• Based on the situation, it may be the company who’s responding who answers the question or an Insurance Broker may answer the questions on behalf of that Broker’s client

• Assuming company wishes to get more information on insurance offerings available to them, they would then proceed to completing the more comprehensive application

• Key is to keep them informed of their progress throughout the application cycle, provide insights into the meaning of all of the unfamiliar terms and acronyms, make it as simple as possible

• Provide results in an easy-to-understand format, measurable, company can see dashboards which break results down in easy-to-digest way, can create and save reports and scorecard
Cyber COPE®
CYBERSECURITY
ASSESSMENT
SAMPLE
SCORECARD
Overall Cyber COPE® Risk Score

Current Score: 42%
Average Industry Score: 59%

1. **60%**
   - Ensure your Organization is ready to identify and respond to a cyber-attack

2. **40%**
   - Ensure your Organization has visibility into real-time activity on their network & systems

3. **50%**
   - Your Organization regularly tests the defences

4. **40%**
   - Your Organization has clearly defined roles & responsibilities

5. **20%**
   - Your Organization has proper documentation
Results by Cyber COPE® Category

- Components: 60%
- Organization: 70%
- Protections: 40%
- Exposures: 30%

0-30% | 31-69% | 70-100%
Your Current Maturity Aligned To Lifecycle

- **Plan**: 32 Requirements
- **Implement**: 27 Requirements
- **Validate**: 9 Requirements
- **Manage**: 21 Requirements

**Cyber Security Lifecycle**
How Ready Are You To Implement Other Security Frameworks?

- PCI: 59%
- NERC CIP: 21%
- NIST CSF: 22%
- CIS CSC: 34%
- OSFI CSA: 68%
Changing Insurance from Static/Reactive to Proactive

• Current approach to security: answer some questions once, get a quote, buy insurance

• Proposed approach with Cyber COPE®: Make it useful and beneficial to answer and update the questions and responses more often, possibly quarterly or semi-annually

• Provide incentives for companies to do so (either lower limits, higher rates or deductibles if they don’t, or higher limits, lower rates or deductibles if they do and can demonstrate they have taken measurable steps to improve their overall risk posture)

• Make the insurance process more proactive, providing guidance so that companies can reduce their risk to minimize breaches; benefits the insurance companies (fewer claims), benefits the clients (fewer breaches)

• Use Insurance products as a reason for companies to become more aware of their exposures and ideally better manage their risk. Insurance costs are often of interest to the Board of Directors, so finding ways to improve them can result in greater Board engagement in the entire process.
Key Things to Remember

• The Cyber world is changing: use these changes as an opportunity to improve your overall risk posture while at the same time gaining a better understanding of how to protect your organization.

• A lot of small changes really can improve your overall risk score; you have to start somewhere, have a plan and have a way of measuring progress.

• Approach cybersecurity thinking of it as a lifecycle; it never ends, you will be at different places in the lifecycle at different times and for different activities.

• Security is not absolute, but the planning you do now and the efforts you take can and WILL make a difference!

• Cyber insurance is part of an overall enterprise risk management strategy – target harden and pre-plan the elements of your response, transfer the financial risk; and then when an event happens activate your plan and engage with your Cyber insurer.
Chubb. Insured.