Cyber COPE®

Transforming Cyber Underwriting
by Russ Cohen

CHUBB®

"How tall is your office building?"

"How close is the nearest fire hydrant?"

"Does the building have an alarm system?"

Insurance companies ask simple, objective questions like these so they can provide you with adequate coverage, but still limit their financial losses.

But what kind of questions do insurance companies ask if you need cyber insurance? Do you know if your company encrypts all its sensitive information, has firewalls at all Internet access points, or patches computer systems for all known vulnerabilities? Do you even know who to ask?

The answers to these and other cyber-related questions are often complex and subjective. This lack of simplicity and objectivity makes evaluating your company's cyber risk very "risky" for insurers, which makes it harder for you to get the coverage you need. If the number of floors in your building or the age of your sprinkler system can be used to help assess your commercial property risk, why can't the number of computers in your company be used to more accurately assess your cyber risk? The answer is, it can—by applying COPE, a time-tested property underwriting model, to technology to improve the overall quality of cyber underwriting and data intelligence.

COPE: The Basic Elements of Property Underwriting

Close your eyes for a few seconds and picture any building in your mind. Can you estimate the square feet? Do you know what type of company uses the building? Does it have an alarm system? Is it near a major airport?

It's ok if you don't know the answers, but you probably understand the questions. Responses to questions like these have provided the basic data elements that property underwriters have used to analyze risk for nearly 300 years.[1]

In property underwriting, COPE stands for Construction, Occupancy, Protection and Exposures. Each letter represents a group of data points that contributes to evaluating the overall risk of a particular structure. *Construction* refers to data such as the materials, square footage and the age of a structure, while *Occupancy* refers to what the company does and how the company manages the hazards associated with what they do. *Protection* measures the factors that can help mitigate various types of structural exposures, and *Exposures* describes the potential exposures related to a particular property.

So now imagine a simple three story building. It's made of mainly steel and brick. Four businesses use the building, employing approximately 20 workers each. The building has a central sprinkler system, an alarm system and meets all other building codes. It is located in a wooded office complex in San Diego, California. Although a lot more information than this is needed to produce an actual insurance quote, the COPE model is highly effective for gathering and organizing information for a property underwriter to effectively evaluate a property risk.

But what makes the COPE model so effective?

Underwriting can be as much of an art as it is a science. This is because it requires analyzing both objective measurements ("the science") and subjective measurements ("the art"). One of the key benefits of the COPE model is that it enables a property underwriter to leverage both the objective measurements of *Construction* and *Occupancy* with the subjective measurements of *Protection* and *Exposures* to make a better decision about a risk.

Another key benefit is the public accessibility of data. Companies specialize in gathering and analyzing this data for commercial properties. Over the years, insurers and reinsurers, corporations, financial institutions and governments have shared their data with these organizations, recognizing that, by working together, they can better manage global catastrophic risks.

When an underwriter looks at a building that is made of 75 percent wood (objective) and has a fire suppression system that is 20 years old (subjective), he/she is able to weigh these facts together and compare it against historical data to determine the risk that contributes to the overall pricing of a policy. By looking at the subjective data, the underwriter also has the opportunity to improve a policyholder's risk – i.e., "You may want to upgrade your sprinkler system."

Combining Art and Science in Cyber Underwriting

As we have seen, COPE is a straightforward and effective method of examining diverse measurements to help underwriters make better decisions about property risk. So how can COPE be applied to technology to improve the overall quality of cyber underwriting decisions? First, it must be simple enough that individuals with both technical and non-technical knowledge can use it. Second, it must provide both objective and subjective measurements, in line with the original COPE model. Finally, it must foster information sharing so that organizations can learn from each other to help mitigate future losses.

The result is Cyber COPE® – a new model for cyber underwriting, intended to simplify and improve the assessment of both cyber and privacy risks.

Transforming COPE to Cyber COPE®

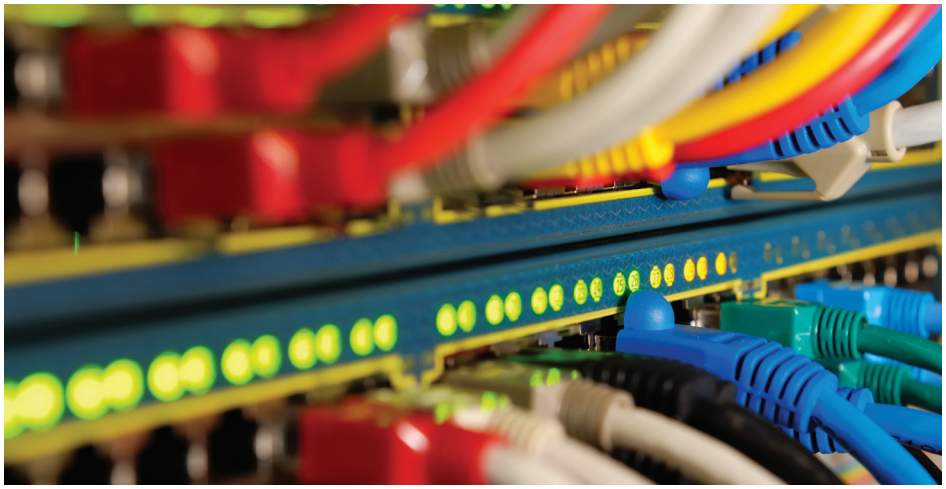
To apply the COPE methodology to cyber exposures, we start by changing *Construction* to *Components*. Similar to a physical building, *Components* represents the objective data elements that provide information on the overall cyber "structure" of a company, such as the number of computers, user accounts and Internet connections.

Next, we convert *Occupancy* to *Organization*. Similar to the make-up of the company, Organization captures the objective data elements related to the people, process, information and overall enterprise risk strategy of an organization. This might include the company's industry, number of employees, number of contractors and budget allocations for cyber security.

The last two elements of the COPE model, *Protection* and *Exposures*, remain the same. However, instead of property, the aim is to capture the subjective data elements that describe a company's cyber defenses *(Protection)* and potential cyber weaknesses *(Exposures)*. Examples of *Protection* elements can include encryption, firewalls and intrusion detection, while examples of *Exposures* can include threat actors, system errors and software vulnerabilities.

Figure 1 - The table below summarizes this transformation of COPE to Cyper COPE®:

COPE	Cyber COPE®	Measurement Type	Sample Data Elements
Construction	Components	Objective	Number of endpoints and network connections, software versions, and data center locations
Occupancy	Organization	Objective	Policyholder's industry, quality of IT and security related policies, and use of industry standards
Protection	Protection	Subjective	Data retention policies, firewalls, monitoring, and incident response/response readiness policies
Exposures	Exposures	Subjective	Political or criminal motivation, types of outsourcing, and type/amount of sensitive information



Components

What are the data elements that make up the cyber "structure" of a company? When assigning elements to the *Components* category, it is important to understand that the data must be as objective as possible. Therefore, for each element, the goal is to measure it against the simplicity of the question, "How many floors are in a building?" This question provides objective data, and is also simple enough for everyone to understand. The following questions are examples of the type that would provide measurable data elements for *Components*:

- How many employee user accounts or "IDs" do you have?
- How many non-employee user accounts do you have?
- How many public Internet connections does your company have?
- How many third parties do you use to store or process your company's information?
- How many endpoints (e.g., desktops, laptops or mobile devices) are used by your company?

Accessibility, that other key factor of property underwriting, is also important here. Companies are starting to share their data with third parties so that data can be analyzed to help lessen cyber risk as a whole. As this trend grows and more companies are able to access the data, the industry as a whole will be better equipped to assess risk and work together to lessen exposures in the future.

Organization

The data elements captured in *Organization* are more straightforward than those in *Components*, although these elements must also be as objective as possible for the model to be effective. With *Organization*, the goal is to gather data that give the underwriter a Board-level or enterprise view of the company's cyber vulnerability. The questions posed for *Organization* are also framed against the "number of floors in a building" question to help drive objectivity:

- What is your company's primary industry?
- Which industry security standards do you leverage?
- Do you have specific security language built into third party agreements?
- What PCI merchant level is your company?
- What percentage of the IT budget is allocated to cyber security?

Protection

The data elements captured in *Protection* concentrate on the security controls that exist within a company to help prevent against a cyber incident. These data elements are reminiscent of those found in existing security standards, such as the NIST, PCI and ISO27001. Although it would be easy to insert questions from these standards into an application for cyber insurance, they are far too lengthy for organizations, especially smaller ones, to complete. Additionally, few insurance companies, brokers or agents will have sufficient resources to assess all the data points provided by these standards.

Therefore, the *Protection* data elements are based on a core set of refined security controls. Although new types of attacks occur all the time, the same vulnerabilities are still exploited year over year. For example, ransomware is a new type of malware that restricts access to files unless a ransom is paid to the attacker. However, ransomware is generally only effective if someone clicks a malicious link in an email (i.e., an untrained person is exploited). This is the type of risk that a company can mitigate through proper training and education.

The goal of *Protection* is to decide which security controls are essential for all companies, while also permitting a degree of subjectivity. Because the objective data elements of *Components* and *Organization* are captured first, the subjective elements of *Protection* are first identified as simple terms, enabling the underwriter to develop subjective questions as they gather additional information. Sample terms and questions include:

1. **Awareness:** how often are your employees trained on cyber security?
2. **Authentication:** do you use and enforce password hygiene?
3. **Encryption:** is your sensitive data encrypted at-rest and in-transit?
4. **Firewalls:** do you limit ports on all Internet access points?
5. **Anti-Malware:** what anti-malware software do you install?
6. **Systems management:** do you have any unsupported software running?
7. **Account management:** do you restrict access based on job function and responsibilities?

These terms are numbered because it is also important to prioritize the elements gathered here. For example, statistically, humans are the weakest link in cyber security. By focusing more questions on security awareness programs and authentication, you're also prioritizing your loss control investment.

Exposures

When we think of *Exposures* in property, we think of things like natural disasters, fire, floods, theft, etc. To mimic that methodology for Cyber COPE®, we have to understand the underlying characteristic of a cyber exposure, then determine which ones apply to any particular company.

The primary characteristic is that these exposures generally cannot be controlled. For example, in property, we can try to predict where a hurricane might strike, but we have no control over the hurricane itself. Relatedly, for cyber, we can try to predict which company a hacktivist might target, but we have no control over the hacktivist's motivation or determination.

By sharing information and developing a common underwriting foundation, the industry will be better equipped to protect organizations from cyber-related exposures.

Since these are more subjective measures, the elements captured for *Exposures* are presented as simple terms rather than leading questions:

- **Handling of desirable information:** corporate data, customer data
- **Targeted attacks:** motivated threat actors
- **Non-targeted attacks:** unintentional human errors
- **Third-party resources:** outsourcing
- **Common software vulnerabilities:** Java, Flash, Windows
- **System/software errors:** programming errors
- **Compliance or regulatory requirements:** PCI, HIPAA

As an example, let's look at the first component identified, *Handling of Desirable Information*. Ideally, a company can control access to this type of data. But if you store/process millions of credit cards, you may outsource that function to a third party processor. The exposure still exists, but the protection is no longer within your control. And if multiple companies use the same payment processor as you, your exposure increases significantly due to risk aggregation. This is particularly true for your insurance carrier.

Cyber COPE®: A New Era for Cyber Underwriting

In the 1700's, the risk of fire made it difficult for many commercial property owners to secure the insurance coverage they needed; over time, the industry adopted the COPE concept. Fast forward to modern times, and the risk is cyber – where the losses are so high, and the threats seem to change so quickly, that companies are once again struggling to secure the coverage they need.

The COPE methodology has been effective because it uses simple, straightforward questions to gather both objective and subjective data to more accurately assess risk. It has withstood the test of time because of the collaborative efforts of numerous parties to share and analyze the data gathered, using that analysis to identify weaknesses in advance so companies can better protect their investments in the future.

Likewise, Cyber COPE® has been designed to be simple to use and to provide the right balance of objectivity and subjectivity for the underwriter. Moreso, it provides a path forward for the cyber insurance industry to begin to break down the historic barriers common with information sharing. By sharing information and developing a common foundation in which to underwrite constantly evolving cyber risks, the industry will be better equipped to provide the proper coverage and solutions to protect organizations from cyber-related exposures.

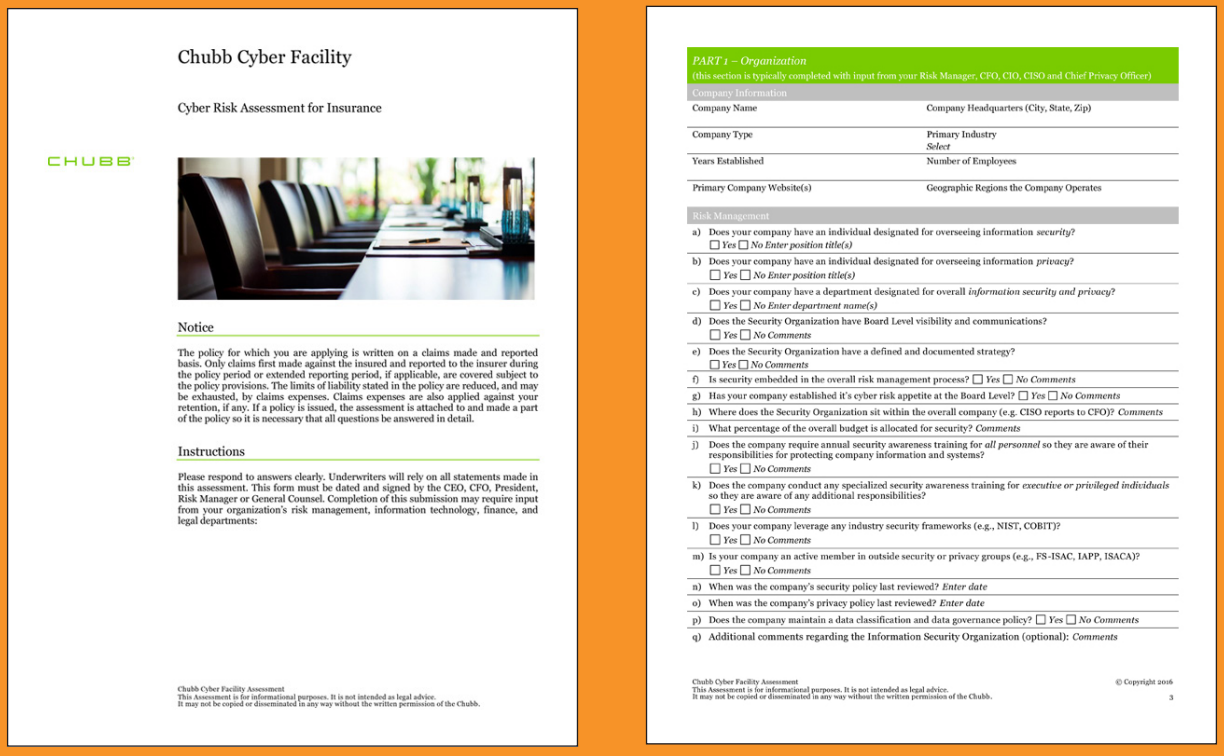
Implementing Cyber COPE®

Cyber COPE® was first leveraged as the basis for the insurance application for Chubb's Global Cyber Facility, which helps companies assess their cyber and data privacy risk, incorporates loss control services to mitigate losses, provides access to post-incident services and offers up to $100 million in primary capacity – all in a single policy purchase. To implement Cyber COPE®, Chubb worked with strategic allies within the cyber security industry to develop a set of questions that provides the necessary data elements to help underwriters comprehensively assess cyber risk.

Determining which data elements could be considered a *Component*, where we needed to balance both objectivity and accessibility, proved to be challenging. Identifying the data elements within *Exposures* also proved to be challenging due to the number of potential threats a company could face. However, we felt it was important to be as broad as possible in terms of threats in order to promote a deeper discussion with policyholders, including raising the awareness of potential exposures that might not have been considered by the policyholder in the past. This also helped determine loss control opportunities.

In contrast to *Components* and *Exposures*, determining the data elements for *Organization* and *Protection* was less challenging because they were fairly well known. Here, we were challenged to reduce the number of questions to ensure the underwriting process wasn't significantly time-consuming and could incorporate the flexibility needed when underwriting larger organizations. To achieve this, we structured the questions to address the needs of a top-down organization. Board-level questions are presented first, followed by questions for C-level staff (e.g., CIO, CFO, CISO) and, lastly, the more specific and technical questions for senior management level staff, such as Information Security Officers, senior counsel, and security operation managers.

The Cyber COPE® model presents significant opportunities for innovation within cyber underwriting, particularly within the *Components* and *Exposures* categories. We continue to collaborate with industry leaders to refine objective measurements that correlate to specific cyber risk exposures. This type of collaboration is critical in identifying what will be most impactful to lessen the risk of cyber attacks. All organizations can benefit as we work together to gather and analyze data to better predict the frequency and severity of cyber attacks and risk aggregation.



Chubb Cyber Facility

Cyber Risk Assessment for Insurance

CHUBB

Notice

The policy for which you are applying is written on a claims made and reported basis. Only claims first made against the insured and reported to the insurer during the policy period or extended reporting period, if applicable, are covered subject to the policy provisions. The limits of liability stated in the policy are reduced, and may be exhausted, by claims expenses. Claims expenses are also applied against your retention, if any. If a policy is issued, the assessment is attached to and made a part of the policy so it is necessary that all questions be answered in detail.

Instructions

Please respond to answers clearly. Underwriters will rely on all statements made in this assessment. This form must be dated and signed by the CEO, CFO, President, Risk Manager or General Counsel. Completion of this submission may require input from your organization's risk management, information technology, finance, and legal departments:

Chubb Cyber Facility Assessment
This Assessment is for informational purposes. It is not intended as legal advice.
It may not be copied or disseminated in any way without the written permission of the Chubb.

PART 1 – Organization
(this section is typically completed with input from your Risk Manager, CFO, CIO, CISO and Chief Privacy Officer)

Company Information

Company Name	Company Headquarters (City, State, Zip)
Company Type	Primary Industry *Select*
Years Established	Number of Employees
Primary Company Website(s)	Geographic Regions the Company Operates

Risk Management

a) Does your company have an individual designated for overseeing information *security*?
☐ *Yes* ☐ *No Enter position title(s)*

b) Does your company have an individual designated for overseeing information *privacy*?
☐ *Yes* ☐ *No Enter position title(s)*

c) Does your company have a department designated for overall *information security and privacy*?
☐ *Yes* ☐ *No Enter department name(s)*

d) Does the Security Organization have Board Level visibility and communications?
☐ *Yes* ☐ *No Comments*

e) Does the Security Organization have a defined and documented strategy?
☐ *Yes* ☐ *No Comments*

f) Is security embedded in the overall risk management process? ☐ *Yes* ☐ *No Comments*

g) Has your company established it's cyber risk appetite at the Board Level? ☐ *Yes* ☐ *No Comments*

h) Where does the Security Organization sit within the overall company (e.g. CISO reports to CFO)? *Comments*

i) What percentage of the overall budget is allocated for security? *Comments*

j) Does the company require annual security awareness training for *all personnel* so they are aware of their responsibilities for protecting company information and systems?
☐ *Yes* ☐ *No Comments*

k) Does the company conduct any specialized security awareness training for *executive or privileged individuals* so they are aware of any additional responsibilities?
☐ *Yes* ☐ *No Comments*

l) Does your company leverage any industry security frameworks (e.g., NIST, COBIT)?
☐ *Yes* ☐ *No Comments*

m) Is your company an active member in outside security or privacy groups (e.g., FS-ISAC, IAPP, ISACA)?
☐ *Yes* ☐ *No Comments*

n) When was the company's security policy last reviewed? *Enter date*

o) When was the company's privacy policy last reviewed? *Enter date*

p) Does the company maintain a data classification and data governance policy? ☐ *Yes* ☐ *No Comments*

q) Additional comments regarding the Information Security Organization (optional): *Comments*

Chubb Cyber Facility Assessment
This Assessment is for informational purposes. It is not intended as legal advice.
It may not be copied or disseminated in any way without the written permission of the Chubb.
© Copyright 2016
3

Figure 2 - Sample pages from Chubb's Global Cyber Facility Assessment

About the Author

Russ Cohen serves as the Director of Cyber and Privacy Services for Chubb, where he is responsible for managing all policyholder services associated with Chubb's pre- and post-incident cyber services. Mr. Cohen has more than 15 years of cyber security and technology experience in a variety of roles, including an ethical "white hat" hacker. He holds a CISSP certification and is an active member of various security organizations, including Infragard, ISC2, FS-ISAC, and the Cloud Security Alliance. Mr. Cohen can be contacted at Russ.Cohen@chubb.com.

Endnotes

[1] Boggs, Christopher J. (2010). Property and Casualty Insurance Concepts Simplified: The Ultimate "How to" Insurance Guide for Agents, Brokers, Underwriters and Adjusters. (Wells Media Group, Inc.). United States

Chubb. Insured.℠

www.chubb.com/us/cyber

10/2016