CHUBB®

Cyber COPE®

Transforming Cyber Underwriting

By Russ Cohen and Patrick Thielen

"How tall is your office building?"

"How close is the nearest fire hydrant?"

"Does the building have an alarm system?"

"Are you in a flood zone?"

Insurance companies ask simple, objective questions like these so they can properly and thoroughly underwrite risks presented for coverage.

But the kinds of questions insurance companies ask when underwriting cyber insurance are not always so simple.

For example, 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 whom 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 more uncertain for insurers, which makes it harder for you to get the coverage you need and at the proper price point. 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.

Combining Art and Science in Cyber Underwriting

COPE (Construction, Occupancy, Protection, and Exposures) 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 so 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 in order to help mitigate future losses. Basically, it needs to inform society as to what is causing 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, Multifactor Authentication (MFA), and intrusion detection, while examples of *Exposures* can include threat actors, system errors, and software vulnerabilities.

Figure 1

The table to the right summarizes the transformation of COPE to Cyber COPE:

COPE	Cyber COPE	Measurement Type	Sample Data Elements
Construction	**Components**	Objective	Number of endpoints, 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, MFA, 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 elicits objective data and is also simple enough for everyone to understand. The following questions are examples of those that would provide measurable data elements for *Components*:

- How many employee user accounts or "IDs" do you have?
- How many software applications exist in your environment?
- 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 reduce overall cyber risk. 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 reduce 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?
- Which Payment Card Industry (PCI) merchant level is your company?
- What percentage of the IT budget is allocated to cyber security?

Protection

The data elements captured in *Protection* are focused on the security controls that exist within a company to help prevent 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 answer. 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 after year. For example, ransomware is a 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 on a malicious link in an email, fails to secure an Internet-facing open port, or fails to update vulnerable software. This is the type of risk that a company can mitigate through proper training, education, and cyber hygiene.

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. **Incident Response:** do you have an incident response plan that is tested annually, at minimum?
2. **Vulnerability Management:** do you have an ongoing process to identify, assess, and address weaknesses in computing systems?
3. **Patch Management:** do you have a process of installing security updates to applications and system software when provided by the manufacturer?
4. **MFA:** do you have MFA implemented on email systems, remote network access, and applications with sensitive information?
5. **Endpoint Detection & Response:** have you implemented an advanced anti-malware solution that detects and responds to active threats not detected by traditional antivirus software (e.g., zero-days, advanced persistent threats)?
6. **Perimeter Email Security:** do you have software to scan emails and quarantine those that may contain malicious content (e.g., attachments, links)?

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 insurance, we can try to predict where a hurricane might strike, but we have no control over the hurricane itself. Relatedly, for cyber insurance, we can try to predict which company a hacker might target, but we have no control over the hacker's motivation or determination.

Similar to floods and earthquakes, some cyber risks have the potential to become widespread events that affect many policyholders. Future cyber catastrophes have the potential to be even worse than natural catastrophes because cyber events aren't limited by geographic or time boundaries. Accordingly, just as a property underwriter would assess exposures and protections against natural catastrophes and structure coverage accordingly, a cyber underwriter must do the same. And just as a property portfolio manager must ensure that no single event could result in aggregated losses that exceed an insurer's risk appetite, an insurer must likewise objectively quantify and contain cyber systemic risk within its portfolio.

By sharing information, developing a common underwriting foundation, and using a quantifiable coverage structure for widespread events, the insurance 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 Sensitive 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
- Widespread Events: reliance on widely used technologies

As an example, let's look at the first component identified, Handling of Sensitive 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, if the carrier has a large number of policyholders relying on that same vendor.

Cyber COPE: A New Era for Cyber Underwriting

In the 1700s, 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 emerging risk is cyber — where the potential losses are high and the threats 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 assess risk more accurately. 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. Further, it provides a path forward for the cyber insurance industry to begin to break down the historic barriers that prevent information sharing. By sharing information and developing a common foundation on 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.

The Cyber COPE model presents significant opportunities for innovation within cyber underwriting, particularly within the *Components* and *Exposures* categories. We at Chubb 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.

About the Authors

Russ Cohen is Vice President and Cyber and Technology Practice Leader at Chubb, where he helps policyholders analyze cyber exposures and respond to cyber events when they occur. He also drives innovations within cyber underwriting, claims, and actuarial disciplines. Mr. Cohen has more than 16 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 and (ISC)[2].

Patrick Thielen is Senior Vice President, Financial Lines, at Chubb and product lead for the Cyber and Technology E&O lines of insurance for North America. He has been part of the leadership teams that have launched the Small Commercial Insurance division, the Cyber ERM and DigiTech® ERM product offerings, and the Masterpiece® and Blink Cyber Protection products. Mr. Thielen has 20 years of experience in cyber and technology insurance, and is currently leading Chubb's efforts to enhance and expand cyber coverage and risk mitigation solutions for businesses of all sizes, as well as for individuals and their families.

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

2 CyberAcuView (2021): Accessed at https://cyberacuview.com/press-release-june-2021/

Chubb. Insured.℠

www.chubb.com/cyber