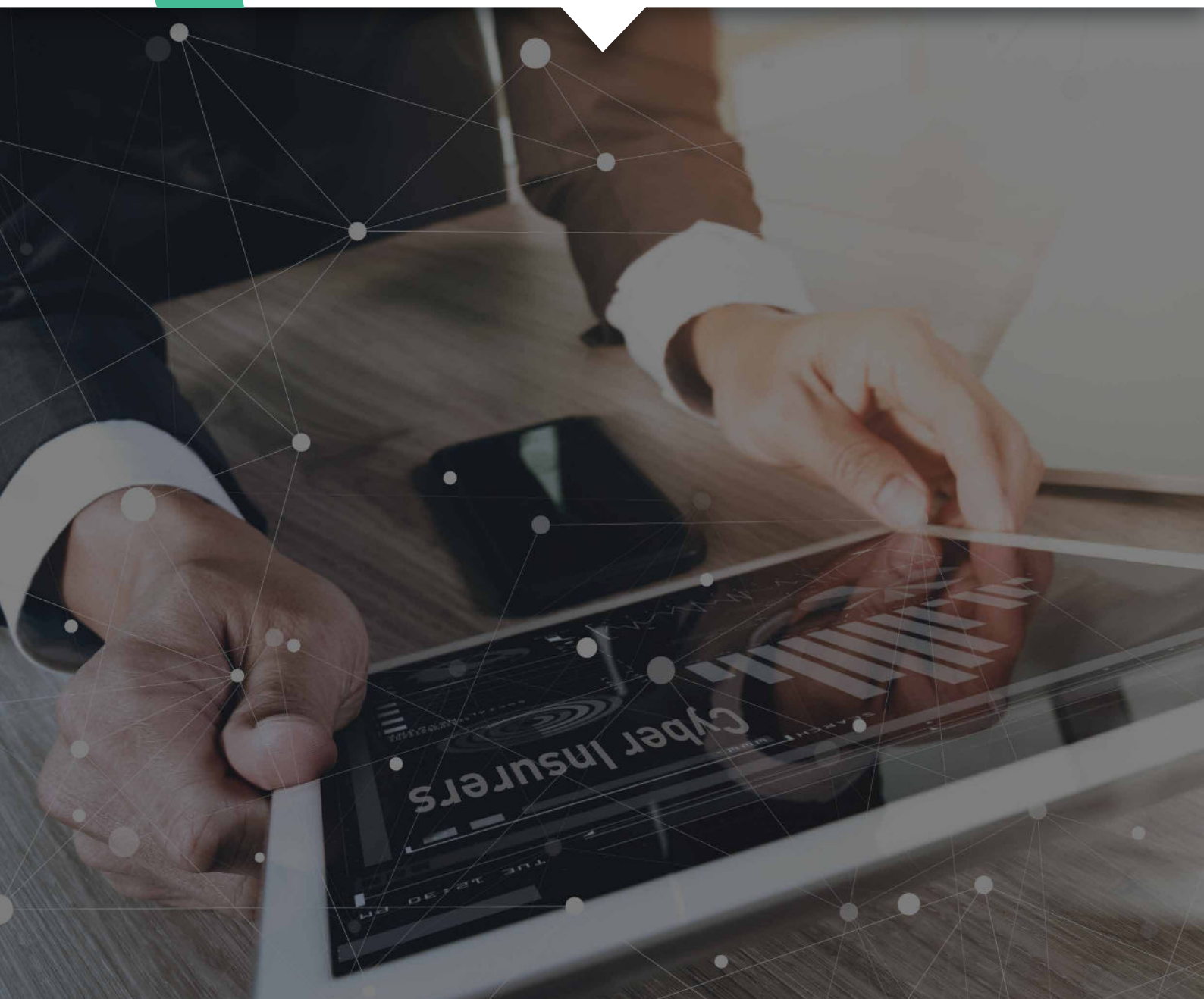
Cymulate
Breach & Attack Simulation

Cyber Insurers

A New Approach in Assessing Cyber Risk



Cymulate

Table of Contents

01 | Introduction 2

02 | Cyber Attackers: As Certain as Death and Taxes 3

- They are Relentless
- They're Agile
- They're Innovative
- They Change Targets
- They Have an Unfair Advantage

03 | What's at Risk for Your Clients? 5

- The Pervasive Unknown
- Costs Associated with a Breach

04 | Calculating Cyber Insurance Risk 7

- Complex Data Relationships
- Getting Accurate Visibility
- Reducing the Cost of "Nonstandard" Variables
- Asking the Right Question

05 | The Cymulate Assessment 10

- Cymulate BAS Increases Risk Assessment Accuracy

06 | About Cymulate - BAS Made Simple 11

01 | Introduction

As cybercriminals continuously change their targets and attack techniques, the impacts ripple out across operations, security defenses, and ultimately, organizations' bottom lines. In 2019, organizations were 31% more likely to experience a breach within two years than they were in 2014 [1]. As risk increases, so do associated costs. For enterprise organizations, the average total cost of a data breach now stands at $3.92M [2]. Worse, costs continue to affect a breached organization for several years after the breach is contained.

For insurers, cyber insurance offerings can add value to existing business clients' policies and generate incremental revenue. However, accurately assessing cybersecurity risk for any given client is challenging at best. Currently, insurers rely on questionnaires, penetration tests, and onsite assessments to estimate the cybersecurity posture of applicants, which is both time consuming and expensive.

Since global IT security skills shortages are significant[3], there is also a lack of specialized and qualified personnel that have the experience and expertise to perform cyber risk assessments. This paper describes the unique attributes of cybersecurity risk, provides insight into clients' risk assessment challenges, and offers a new way to measure clients' risk based on real-time, continuous assessment of their security controls.

[1] Cost of a Data Breach Report 2019, IBM Security and Ponemon Institute
[2] Cost of a Data Breach Report 2019, IBM Security and Ponemon Institute
[3] https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops/

02 | Unique Attributes of Cyber Attack Risk

Cyber Attacks: As Certain as Death and Taxes

Cyber attacks have become one of the certainties of business life. In 2017, cybercrime cost the global economy $600B[4]. In 2019, the figure rose to $2.9M globally every minute—resulting in $1.5 trillion in costs by the end of 2019. Cyber attackers represent a highly fluid risk for these reasons:

They are Relentless

Adversaries are relentless in their pursuit of a security gap or error. They never stop, knowing that time and human nature eventually work in their favor.

They're Agile

It's a race that attackers are winning. Almost 80% of organizations are introducing digital innovation faster than they can secure it against cyber attack[5].

As defenders become better at identifying intrusions, attackers have become faster in order to achieve their goals before detection. They identify security gaps much faster than in the past and once they initially breach a company's defenses, they can "break out" moving laterally in the network very quickly. For example, a recent study found that Russian adversaries "break out" on average just 18 minutes after initial entry[6]. The ability to move faster than defenders further increases risk of serious damage to the breached organization.

They're Innovative

Every day, cybersecurity researchers identify new threats in the wild. Attackers also continuously vary their bag of "tried-and-true" tactics. For example, attackers originally used phishing emails to transmit GandCrab ransomware and infect systems. In the first nine months of 2018, GandCrab was updated five times[7]. It continues to evolve—now able to avoid detection, bypass security solutions, and trick victims into installing it onto their systems.

They Change Targets

Adversaries increasingly change targets to establish and exploit connections. Even in organizations with robust security controls, attackers have breached supplier or service provider networks and used it as a route into the target organization's network[8]. Many highly publicized breaches in 2018 were the result of supply-chain attacks, such as the company in Figure 1.

Supply Chain Attack Exposes 11.9 Million Records[9]

Quest Diagnostics, an American Fortune 500 clinical laboratory company, said that a web payment page on its billing collection vendor's website was accessed by an unauthorized user between August 1, 2018 and March 30, 2019. The information on the American Medical Collection Agency's (AMCA) affected system included medical information, financial information such as credit card numbers and bank account information, and other personal information like Social Security Numbers. Figure 1: Supply chain attack on healthcare organization

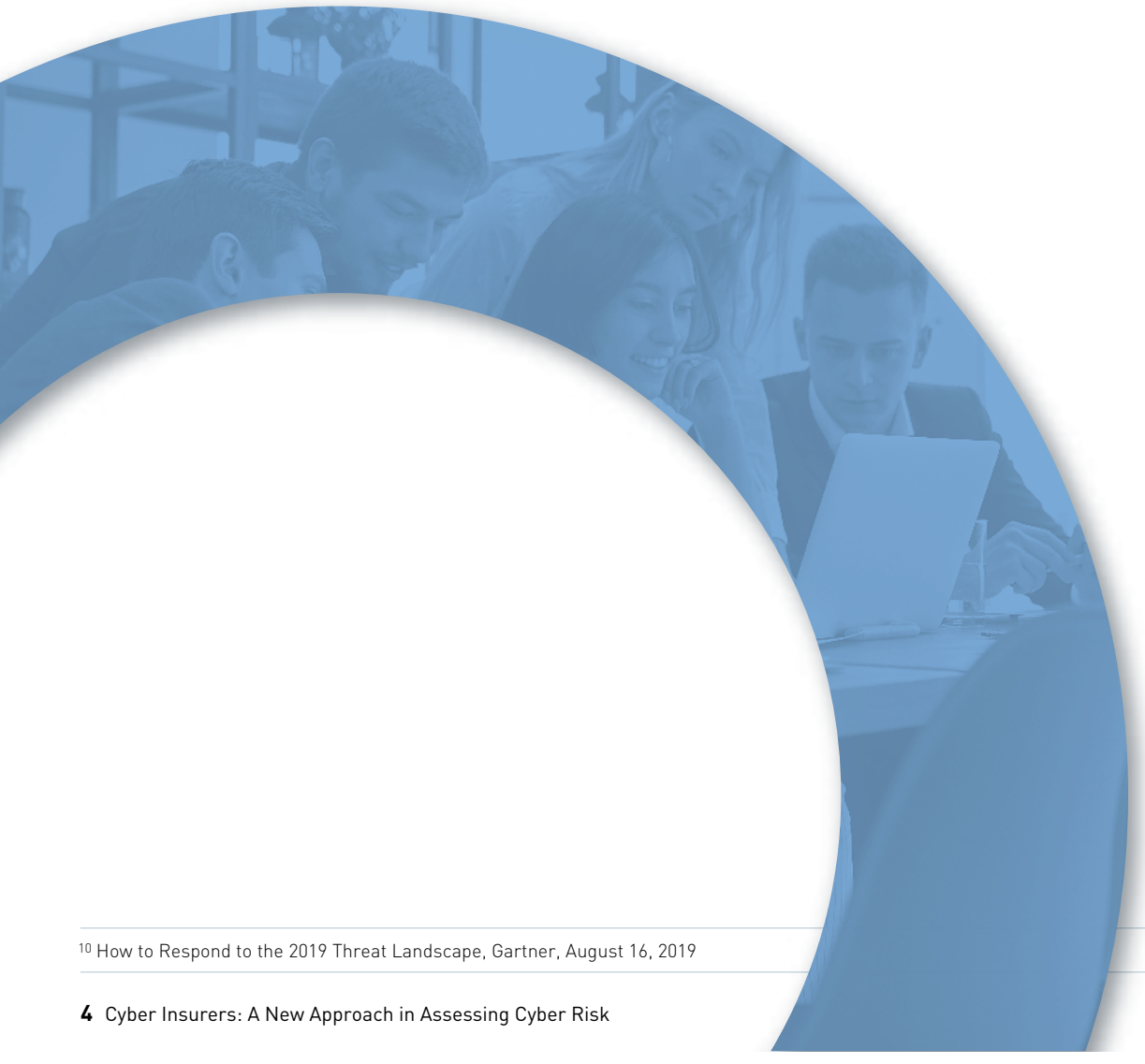
4 Cybercrime Costs the Global Economy $2.9M a Minute, August, 30, 2019 https://www.technology.org/2019/08/30/cybe crime-costs-the-global-econ my-2-9m-a-minute/
5 Ninth Annual Cost of Cybercrime Study, Accenture, conducted by Ponemon, 2019; https://www.cmswire.com/information-management/the-cost-of-a-cyber-breach/
6 2019 Global Threat Report, Adversary Tradecraft and the Importance of Speed, Crowdstrike
7 Old Threats are New Again, Dark Reading, 5/21/2019, https://www.darkreading.com/perimeter/old-threats-are-new-again/a/d-id/1334731
8 How to Reduce the Impact of Supply Chain Attacks by Cybersecurity Procedures, DZone Sept. 4, 2018 https://dzone.com/articles/how-to-reduce-the-impact-of-supply-chain-attacks-b
9 The 13 Biggest Data Breaches of 2019 (So Far), CRN.com https://www.crn.com/slide-shows/security/the-13-biggest-data-breaches-of-2019-so-far-/1

In April 2019, Docker, a leading provider of enterprise-grade container platforms and services, was hacked. Although the breach wasn't numerically large, compromised data included developer GitHub usernames, hashed passwords, and Github and Bitbucket tokens. Nearly all users of the compromised Docker Hub database are developers in large enterprises. That means large enterprises - the covered entities under a cyber insurance - now have internal DevOps teams whose credentials are compromised, giving cyber attackers easy access to critical R&D work, intellectual property, and new channels for moving laterally within the company. A breach like the Docker breach immediately elevated the risk to these developers' employers.

They Have an Unfair Advantage

Most adversary groups have a huge unfair advantage - with vast amounts of money and skilled resources, they have all the time they want to conduct reconnaissance and identify new exploits.

"If nation states target your organization, they will get in," said Jeremy D'Hoinne, Analyst for Gartner.[10] "The challenge becomes recognizing these sophisticated attacks early, and disregard trying to find all the ways these attackers may enter."



[10] How to Respond to the 2019 Threat Landscape, Gartner, August 16, 2019

03 | What's at Risk for Your Clients?

Client Environments

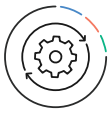
An organization's size and risk posture directly affect its ability to withstand cyber breaches. In 2019, the most-attacked companies were small and medium-sized businesses (SMBs). For an SMB, a breach can mean shutting the doors[11]-78% of small businesses hit by ransomware never recover.

Healthcare organizations, public sector entities, and financial companies, were the next-most attacked industries[12].Healthcare organizations have the highest costs associated with data breaches at $6.45 million - over 60 percent more than the global average[13] of all industries .

The Ninth Annual Cost of Cybercrime Study[14]found the value at risk for an average G2000 company - with 2018 revenues of US $20 billion - equals 2.8% of revenues per year. Regardless of industry or company size, each face two common challenges: the unknown and high costs.

The Pervasive Unknown

Even with the most comprehensive security controls and processes in place, security pros still have a nagging fear that a threat they never heard of has evaded their defenses. There are good reasons for this concern, and many of them are beyond the security team's direct control.



Nonstop change

Organizations' IT systems, business models, markets, partners, employee base, and many other factors change continuously. Nonstop change makes it difficult to keep defenses constantly aligned with the attack surface.

Complexity

On average, enterprises rely on 80 security products .[15] It's difficult to know if-or how well-current configurations, policies, and control settings are delivering enough protection.

Limited resources

Security teams must work within budgets and security expertise is scarce, making it difficult for even large companies to staff operations adequately. Constrained resources directly impact affect an organization's security posture.

Limited assessment capabilities

Even enterprises relying on vulnerability scanning, pen testing, and red teaming still have limited threat visibility. Results depend on individual skills of testers. Testing is usually conducted in a controlled environment, does not cover all elements of each system, and rarely uses the latest Tactics, Techniques, and Processes (TTPs) that real attackers use. Point-in-time snapshots can't keep up with neither the dynamic nature of the threat landscape nor the evolving attack surface of the business.

[11] 'Pandemic Crisis' of MSP Ransomware Attacks Will Grow in 2020, Experts Say, CRN, Oct. 4, 2019; https://www.crn.com/news/channel-programs/-pandemic-crisis-of-msp-ransomware-attacks-will-grow-in-2020-experts-say
[12] 2019 Data Breach Investigation Report, Verizon
[13] Cost of a Data Breach Report 2019, IBM Security and Ponemon Institute
[14] Ninth Annual Cost of Cybercrime Study, Accenture, conducted by Ponemon, 2019; https://www.cmswire.com/information-management/the -cost-of-a-cyber-breach/
[15] Are there too many cybersecurity companies? HelpNet Security, March 30, 2018, https://www.helpnetsecurity.com/2018/03/30/too-many-cybersecurity-companies/

Costs Associated with a Breach

Every company that is breached faces high associated costs, some of which can be felt for years after an incident. The 2019 Cost of a Data Breach Report identified the following factors related to breach costs:

- Lost business, including downtime and business disruption: The average cost of lost business was $1.42 million. On average, breaches caused abnormal customer turnover of 3.9%. The higher the customer turnover, the higher the lost business cost.
- Long-term costs: Approximately one-third of breach costs occur more than a year after the incident.
- Breach lifecycle time: Breaches with a lifecycle less than 200 days were on average $1.22 million less costly than those with lifecycles over 200 days.
- Fines: Organizations subject to industry, national, and/or state regulations can be fined if they are found to be out of compliance. In some cases, companies also incur extensive litigation costs that can drag out for years.

Small and medium-sized businesses can be hit especially hard by costs after a cyberattack. Post-breach responsibilities range from public relations, consumer notices, and customer credit monitoring costs to forensic analysis, data restoration, legal, regulatory fines, and ransom costs.

04 | Calculating Cyber Insurance Risk

The Insurer's Perspective

Based on the risk they face, organizations increasingly want to be insured against the consequences of cyber breaches, just as they are for other property and casualty events. The share of organizations purchasing cyber insurance has increased from 52% in 2014 to 75% in 2018 .[16]

For insurers, the global cyber insurance market accounted for US$4.2 billion in 2017.[17] It is expected to reach US$21.4 billion globally by 2025, growing at a CAGR of 27.2%[18]. During 2018, the North American market for cyber insurance grew. Direct premiums written grew 12.6% for both standalone and packaged policies and cyber premium volume eclipsed $2 billion for the first time[19]. The average annual cost of cyber liability insurance in the U.S. is $1,501 for $1M in liability coverage with a $10,000 deductible .[20] Cyber policies also have been more profitable or insurers than other lines of insurance - the loss ratio for U.S. cyber policies was about 35% in 2018 .[21]

Industry growth is good news for insurers. However, the dynamic threat landscape and clients' wide-ranging cybersecurity postures significantly complicate insurers' abilities to simulate event sets and fit them into traditional statistical distribution models .[22] Cyber attack trends in one year can change dramatically the next year. For example, iIn 2018, a leading cyber insurer's claims saw losses from business email compromise (BEC) attacks pass ransomware-related losses.

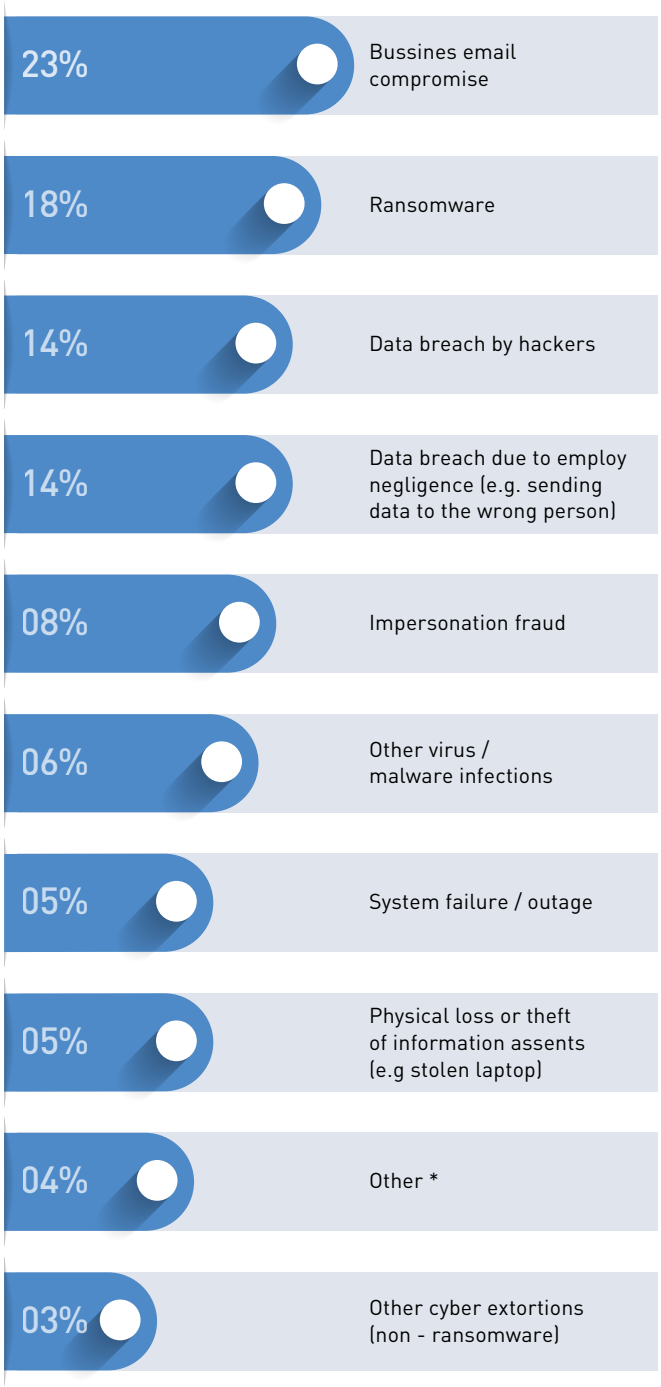


Figure 2: Cyber claims received for clients in EMEA 2018 by the reported incident [23]

[16] Statista.com https://www.statista.com/statistics/422463/ownership -of-cyber-liability-insurance/
[17] Global Cyber Insurance Market Report, Zion Market Research, August 2018 https://www.zionmarketresearch.com/report/cyber- insurance-market
[18] Global Cyber Insurance Market (2019-2025)
[19] Cyber Insurers are Profitable Today but Wary of Tomorrow's Risks, Best's Market Segment Report, June 17, 2019
[20] Average Costs of Cyber Liability Insurance Studied, Business Insurance, September 19, 2019
[21] US Cyber Market Update, 2018 US Cyber Insurance Profits and Performance, Aon, June 2019
[22] Cyber Insurers are Profitable Today but Wary of Tomorrow's Risks, Best's Market Segment Report, June 17, 2019
[23] Claims Intelligence Series, AIG, 2019

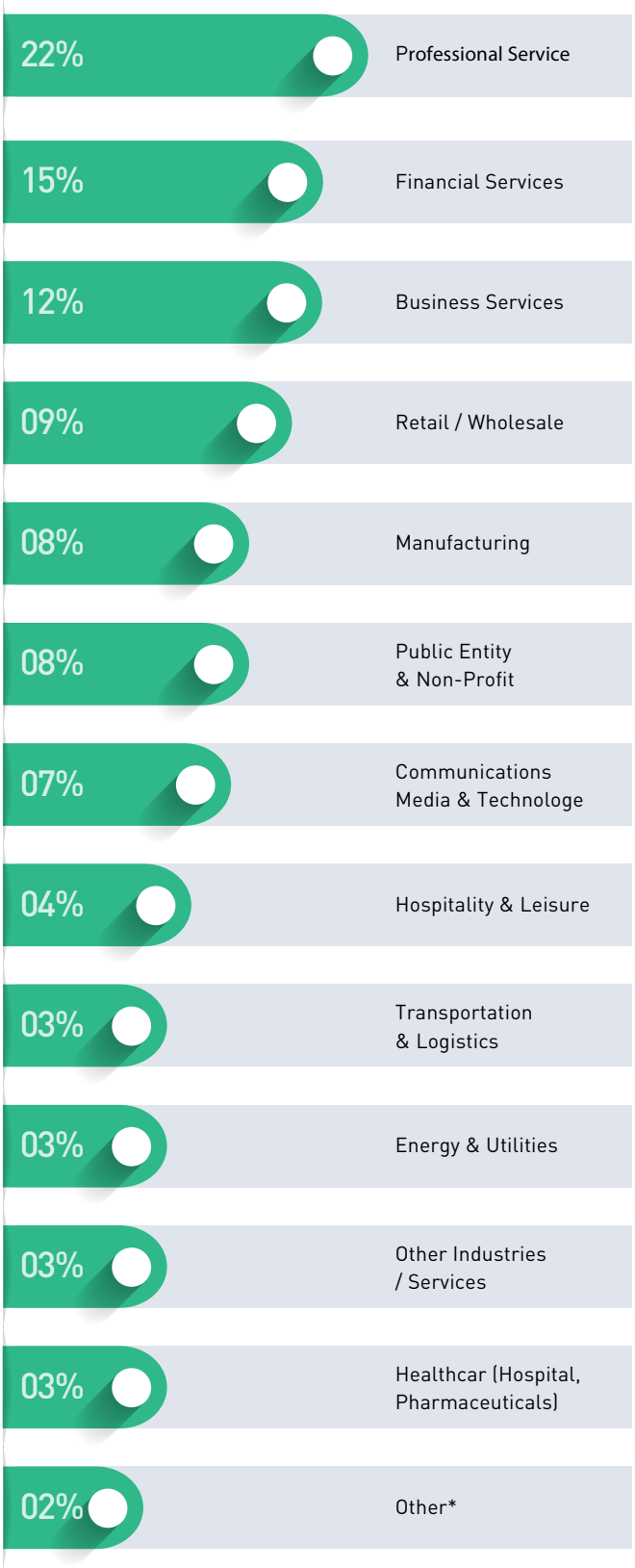


Figure 3: Cyber claims received for clients in EMEA 2018 by industry[24]

Complex Data Relationships

Having as much accurate information as possible is critical to making solid judgments on risk for any given client. The scope of a business, value of its data, annual revenues, and a history of previous cyber breach are all factors important to premium calculations. But more than simply having these facts, it's equally critical to understand the maturity level of clients' security postures. An increase in BEC attacks as shown in Figure 2 must be viewed in light of additional information. In Figure 3, the insurer found that its professional services clients had the highest percentage of claims.

Why is that significant? Professional services firms tend to have less sophisticated security defenses and employees tend to have lower awareness of cybersecurity risks. It makes sense that they would experience a higher level of successful BEC attacks than other industries with more mature security postures.

But even with mature security postures,a single attack can cripple a company, its supply chain, and entire industries. In the NotPetya ransomware attack of 2017, global shipping giant Maersk suffered $300M in damages. That figure only tells part of the story, however. Maersk's New Jersey terminal hosts tens of thousands of shipping containers waiting to be loaded or unloaded and transported by ship or truck. Approximately 3,000 trucks enter and leave the port every day. When NotPetya hit, the terminal gates were frozen shut. Hundreds of semi-trucks were backed up for miles outside. Perishable cargo would rot if not plugged into refrigeration.

[24] Claims Intelligence Series, AIG, 2019

Mission-critical factory components would have to be shipped at exorbitantly higher cost by air. Everything had to be warehoused somewhere in the meantime. Booking systems were down, files with loading and unloading instructions for thousands of containers were wiped away, and cargo owners faced tremendous losses. Worse, the fiasco in New Jersey spread to 17 other Maersk terminals from California to Spain, the Netherlands, and India. Recovery was almost impossible because every domain controller was wiped out, except for one in Ghana. Months later, there were still containers lost in shipyards around the world.

Here are a few examples of major companies hit by the losses; Pharma titan Merck suffered $870M in losses; FedEx lost $400M; French construction company Saint-Gobain lost $384M. And the list goes on. For cyber insurers, a single policyholder victim can represent disaster.

Getting Accurate Visibility

Insurers typically provide a survey or questionnaire to prospective cyber policy clients asking about their cybersecurity defenses. However, a client reporting common defenses such as firewalls, Intrusion Protection Systems (IPS), antivirus, or web application firewalls in place tells an insurer very little about the client's true level of cyber exposure.

Even when an insurer complements the questionnaire with tests and onsite assessments, it still achieves the same results that a client would receive, as described earlier—a point-in-time snapshot limited to specific aspects of the overall infrastructure, policies, and practices. The team does not have visibility into the threat vectors, control effectiveness, or incident response practices across the entire kill chain.

Reducing the Cost of "Nonstandard" Variables

It's costly and time consuming for insurers to send teams to conduct pen testing and other assessments. These are costs incurred before even deciding to approve a policy. Each testing team is different, each client environment is different, and testing strategies vary. How can an insurer determine how much testing, and what kinds, are enough? How much should an insurer spend to determine if a company is worth insuring - or not?

In addition, there are no standards for accurately and universally assessing risk associated with the vast number of security controls in place. These "nonstandard" factors make it nearly impossible to accurately estimate potential losses based on a given threat scenario - or apply consistent judgment across a risk pool.

In 2017, Lloyds of London released a report describing possible outcomes of an extreme cyber attack. In one scenario, a malicious hack takes down a cloud service provider. According to the simulation, the average economic losses from such an attack could range from $4.6B to $53B and could go as high as $125 B depending on the length of time the cloud service was down. In 2019, the firm estimated that a coordinated global cyber attack, spread through malicious email, could cause economic damage anywhere between $85B and $193B a year.

Asking the Right Question

Rather than asking "can an attacker get in?", a better question to ask is "how well are the deployed controls actually working?" This is a question for which an insurer can gain consistent, standard answers across a client's entire infrastructure. Breach & Attack Simulation (BAS) solutions can answer this question and more, such as:

- Are controls working as they are supposed to work and as the client expects?
- Are interdependent controls correctly generating and delivering the right data? For example, are web gateway, firewall, and behavior-based tools correctly alerting the SIEM when they detect suspicious activity?
- Have security control configurations "drifted" over time or been incorrectly set? For instance, are controls actively detecting threats or were they left in monitoring mode?
- If the client has rolled out new technology or a new business process, how has the rollout affected the overall security posture?
- Are controls able to defend against the newest threats and variants?
- Is the client's security team able to identify and respond effectively to alerts?

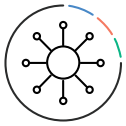
[25] Lloyd's of London calls for cyber cover clarity in insurance policies, July 4, 2019

05 | The Cymulate Assessment

Cymulate breach and attack simulation (BAS) operates from an attacker's perspective to challenge defenses and measure their effectiveness. Easy to use, a member of an insurer's assessment team can simulate attacks on client controls, across vectors, with up-to-the-minute knowledge of immediate threats and tactics. Use BAS to assess email gateways, web gateways, and endpoints for effectiveness against the latest threats.
With just a few clicks, a BAS solution can initiate thousands of simulations to challenge both internal and external defenses.

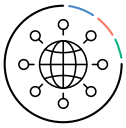
BAS is ideal for benchmarking a client's security posture and using that initial measurement to identify fluctuations in the security posture throughout the period of a policy. At any time, the insurer can assess client status. Quarterly or annual simulations can inform premium and renewal decisions.
Simulation data can document or verify security posture in the event of a claim. Data can be collected across companies and industries for analysis to further refine cyber insurance data models.

BAS Platform Capabilities



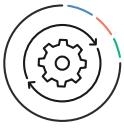
Proven framework
Enables insurers to define the testing approach, plans, and scope.

Industry-recognized threat modeling
Threat models are based on cyber attacker TTPs as described in the MITRE ATT&CK[26] framework



Complete coverage
Challenge controls across all vectors and the entire kill chain.

Metrics
Receive immediate metrics, risk percentages, and attack details describing the full attack story and techniques used.



Repeatability
Benchmark control effectiveness, measure the impact of changes, and continually monitor your risk exposure with standardized data.

Very latest threats
Simulate the very latest cyber attack techniques, supplemented with daily threat data updates.

Uncover third-party and supply-chain gaps
Identify exploitable gaps to provide recommendations for clients and reduce exposure.

Automation for continuous coverage
Automate MITRE ATT&CK-based testing to run daily, weekly, or on demand, depending on testing objectives.

Remediation guidelines
Provide clients BAS remediation and mitigation guidelines and measure remediation progress.

Customizable
Simple wizard-based templates enable you to customize attack simulations to each client's specific needs.

Automate APT testing
Test controls across vectors by emulating logical flow of events as they unfold during a multi-vector APT attack. For example, send a BEC email and automatically launch lateral movement to validate controls when someone clicks.

[26] MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. https://attack.mitre.org/

Cymulate BAS Increases Risk Assessment Accuracy

Cymulate BAS significantly increases accuracy of data used to calculate premiums and risk exposure. By knowing - instead of guessing - the actual effectiveness of a client's security controls, insurers can more easily validate premium levels and evaluate claims.

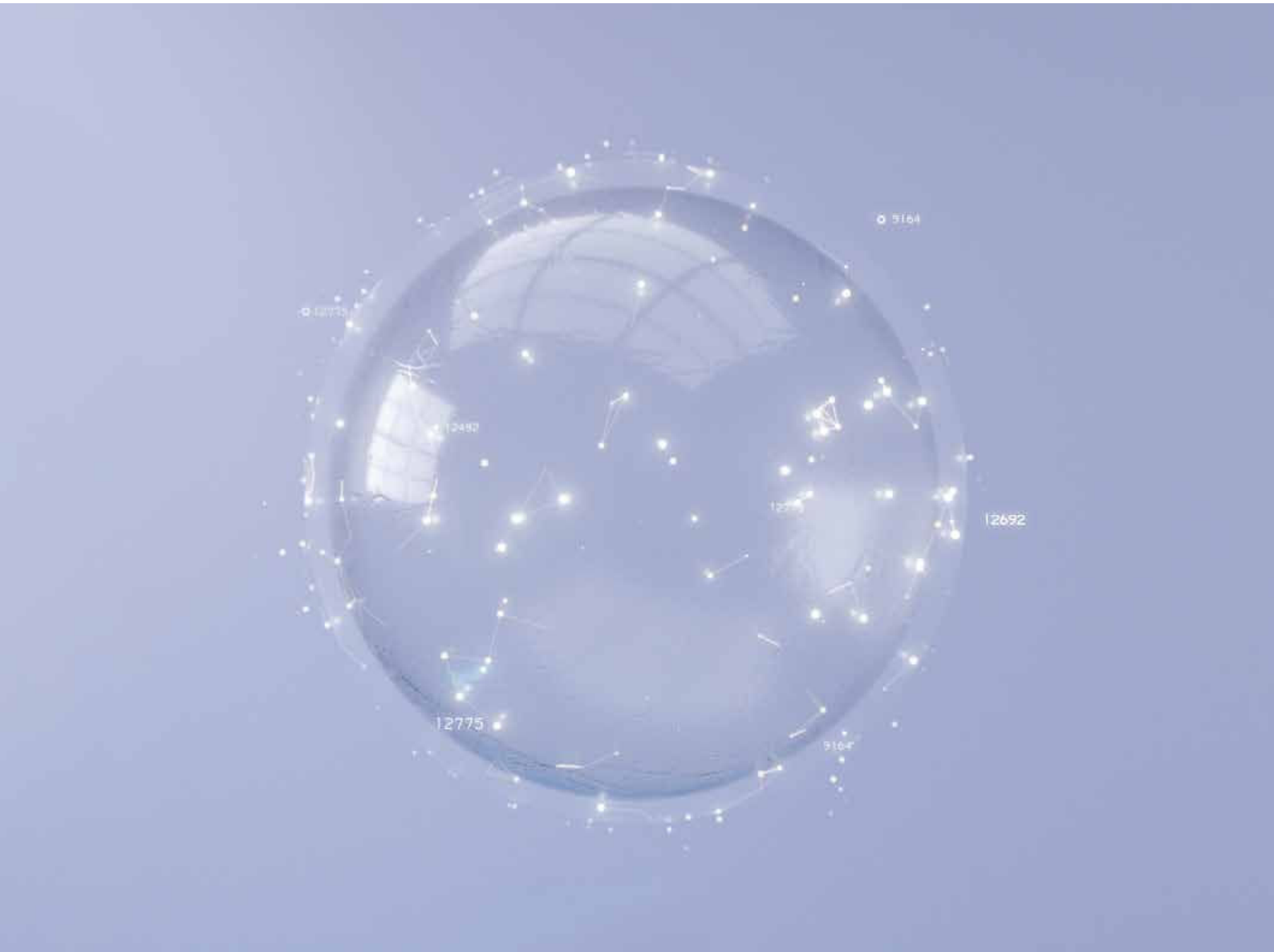
Use Cymulate to:

- Reduce pre-enrollment costs: Easily assess prospective clients' security postures without requiring costly pen testing, advanced security expertise, and lengthy onsite visits.
- Gain consistent, standardized assessment data: BAS delivers clear, risk metrics for each security control as well as across the kill chain, based on the latest threat data, control effectiveness, and other factors. Insurers can benchmark clients' controls and retest annually to document changes for policy renewals.
- Reduce exposure: BAS data can be used with other data analysis tools to simplify risk and premium calculations.
- Reduce investigation costs: Accelerate breach investigations and remediation with the ability to quickly identify attacker TTPs, targets, and specific guidance.
- Increase client satisfaction: BAS testing reports can be given to clients' security teams to provide a clear, documented picture of their security posture. Technical reports help them remediate vulnerabilities and gain deep insight into their risk exposure levels for prioritizing enhancements. Easy-to-read technical and executive-level reporting is available out of the box and can be customized.
- Create new services: With Cymulate BAS, insurers have rich insight and data that can be used to support additional client services.

06 | About Cymulate - BAS Made Simple

Recognized as a **Gartner Cool Vendor** just two short years after its inception, Cymulate's SaaS - based breach and attack simulation platform makes it simple to test, measure and optimize the effectiveness of your security controls any time, all the time. With just a few clicks, Cymulate challenges your security controls by initiating thousands of attack simulations, showing you exactly where you're exposed and how to fix it - making security continuous, fast and part of every - day activities.

Cymulate is trusted by companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision - to make it easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company - and every company - will be.



Ready to Cymulate? Get started with a free trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: 31W 34th Street, 8th floor, New York, 10001 | +1 212 6522632