ARCEO.AI

AN OUTSIZED RISK:

PROTECTING SMALL AND MEDIUM-SIZE ENTERPRISES FROM CYBER RISK

INTRODUCTION

If there is a silver lining in the growing dark cloud of cyber risk, it is that each incident can provide additional information for analysis and insight. The number of cyber incidents occurring at organizations of all sizes continues to increase. The Hiscox 2019 Cyber Readiness Report found that 61% of organizations reported a cyber incident in the past 12 months, up from 45% a year earlier. With expert analysis, each incident presents an opportunity to better understand cyber risks, learn how to mitigate them, and develop effective ways to transfer those risks. In an effort to explore the impact of cyber risk on small and medium-sized enterprises, defined as those with 1,000 or fewer employees, Arceo.ai partnered with Advisen Ltd., one of the leading sources of data for the commercial property and casualty insurance industry. Arceo applied its expertise in data science and insurance to conduct an analysis using Advisen's extensive Cyber Loss Data. The results of that analysis are the subject of this report.

KEY FINDINGS OF ARCEO'S ANALYSIS INCLUDE:

- Cyber incidents have greater impact on small and medium-sized enterprises (SMEs) than on large organizations.
- SMEs take longer than larger organizations to discover breaches.
- Litigation quickly follows disclosure of data breaches.

Arceo's report is the culmination of a collaboration among cybersecurity specialists, actuaries, and experienced data scientists, who worked closely together to obtain an accurate view of what the data shows.

The research was conducted under the supervision of Dr. Ann Irvine, Arceo's Head of Data Science, who framed and described the challenge of the research in the following words: "It's easy to speculate about the frequency and cost of cyber incidents based on anecdotes we hear about in the news. It is equally easy to blindly throw datasets at algorithms and hope for meaningful results. But risk managers, cyber insurance carriers, and others whose business relies on having accurate cyber exposure metrics must take not only a data-driven approach but also must ask the right questions of the data and apply appropriate analytic techniques. Finally, it's equally critical to interpret quantitative results using domain expertise."

WHAT THE DATA AND ANALYSIS SHOW

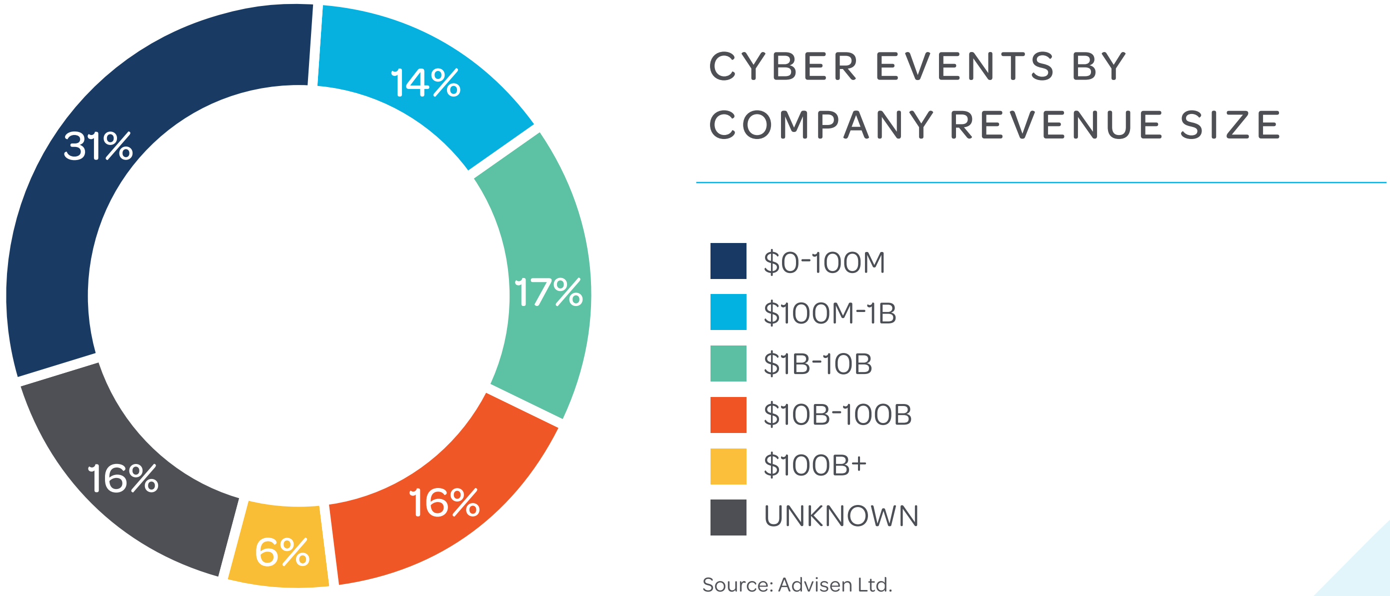
Advisen's 2018 market research discovered that small and medium-sized enterprises represent 90% of new buyers of stand-alone cyber insurance policies. This finding correlates with Arceo's conversations with insurance providers on growth in the cyber insurance marketplace. As this report discusses, Advisen's data and Arceo's analysis confirm that cyber risk has a disproportionately large impact on SMEs. That translates into both a challenge and an opportunity for the insurance industry.

The Advisen Cyber Loss Data is a relational database on more than 95,000 cyber events, which include unauthorized disclosures, thefts or disruptions of customer and employee data, corporate assets, and systems. Advisen utilizes a variety of public and subscription sources to collect current and historical data on organizations of all sizes, including data points on the following: cyber extortion; unintentional disclosure, physical loss or theft, and malicious breach of data; unauthorized data collection and disclosure; identity fraud and fraudulent account access; industrial controls and operations; network and website disruption; phishing, spoofing, and social engineering; and information technology errors.

Advisen's data is enriched with information including the following: case type, case status, affected count, accident date, source of loss, type of loss, actor, loss amount, company size, company type, number of employees, Standard Industrial Classification (SIC) and North American Industry Classification System (NAICS) codes, and geography. Although Advisen points out that its Cyber Loss Data is not a claims database, as it does not include policy-specific information such as deductibles, self-insured retentions, coverage limits, and so on, Advisen's collection is a valuable pool of data for analyzing the impact of cyber events across industries and organization sizes.

For this report, the focus of Arceo's analysis is on SMEs, which account for a significant percentage of the cyber events in Advisen's database. At least 45% of the cyber events Advisen tracks involve organizations with $1 billion or less in revenue (see chart).

CYBER EVENTS BY COMPANY REVENUE SIZE



Source: Advisen Ltd.

ARCEO'S ANALYSIS OF THE ADVISEN CYBER EVENT DATA REVEALED THREE KEY TRENDS:

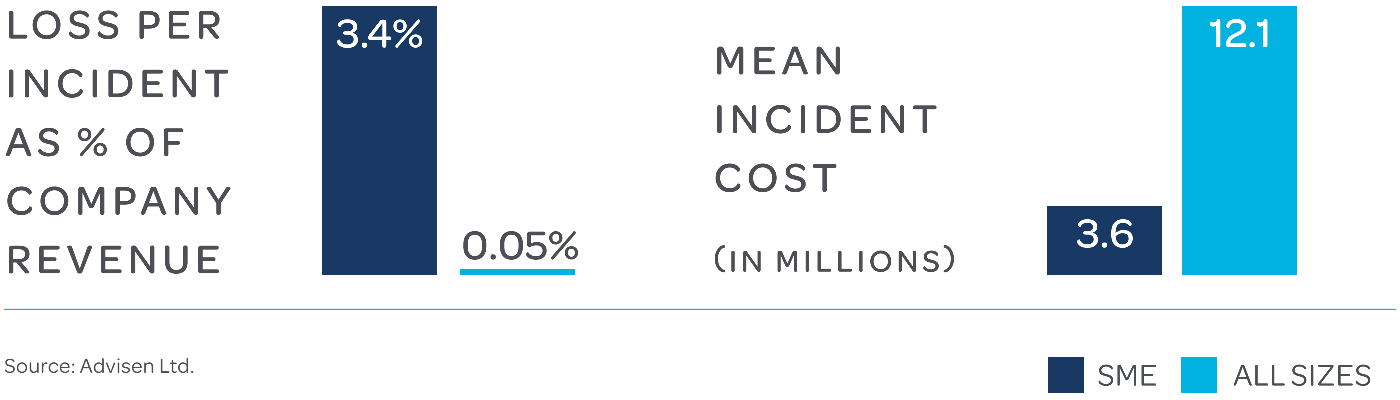
Cyber incidents have a 70 times greater impact on SMEs than on large organizations, when measured as a percentage of revenue.

It takes SMEs up to two years to discover cyber incidents, longer than it takes larger organizations.

Among incidents that eventually result in litigation, 96% land in the court system within a month of disclosure.

SMEs face disproportionately greater cyber exposures than larger entities, studies show. For example, in 2018, 58% of cyber attacks targeted SMEs, according to the Data Breach Investigation Report from Verizon. In addition, the cost of a data breach for organizations with 500 to 1,000 employees is $3,533 per employee, vs. $204 per employee for organizations with 25,000 or more employees, according to the 2019 Cost of a Data Breach Report by IBM Security and the Ponemon Institute.

Another way to measure the impact of cyber events is to examine the costs of such incidents. As Arceo's analysis of the Advisen Cyber Loss Data shows, on average, cyber incidents cost SMEs up to 3.4% of their revenue, or an average of $3.6 million per incident. For small and medium-sized organizations, such costs can wipe out profitability and force them to cancel or postpone business plans. By comparison, the cost of cyber events across all size organizations in the Advisen data set averaged 0.05% of revenue (see chart).



Source: Advisen Ltd.

Cost of cyber incidents for SMEs vs. market overall
Loss per incident includes direct and indirect costs as compiled in the Advisen Cyber Loss Data

Businesses vary widely in their ability to offset unplanned expenses. Larger organizations, for example, may have greater cash flow and access to capital through multiple sources. Small and medium-size enterprises, however, often have thin operating margins and limited resources for raising capital. Therefore, the impact of a cyber event on an SME can be considerable — even before taking into consideration whether the organization has cyber insurance.

This initial finding led Arceo to pursue a deeper analysis of the data to understand the ways in which SMEs were impacted negatively compared with large enterprises. Further analysis found that time is not on the side of small to medium-sized enterprises when it comes to cyber. Arceo's analysis found that organizations with fewer than 1,000 employees not only take longer to resolve cyber incidents, but they also may quickly face litigation after disclosing a cyber event.

DISCOVERY AND LITIGATION

Studies show that the longer it takes an organization to discover that it has experienced a cyber event, the more expensive that incident will be. One reason is that, in the case of a breach, more data can be exposed or lost. This in turn can affect a larger number of individuals, triggering notification requirements and potentially regulatory fines.

Some types of cyber events are recognized quickly. Among those are ransomware attacks, in which malware encrypts data and prevents users from accessing it until a ransom is paid. In the past two years, a spate of ransomware attacks affected cities and school districts, both large and small, across the United States. The city of Baltimore, Maryland, is facing at least $18 million in costs after a May 2019 attack that destroyed some data and forced the city to rebuild its computer system. Atlanta faced a similar attack in 2018 that may end up costing the city more than $17 million. A school district in upstate New York had to delay the start of its school year after a ransomware attack shut down its computer network.

Research shows ransomware remains a growing threat. In the first quarter of 2019, ransomware attacks increased 118%, with perpetrators using 35 new families and innovative techniques to conduct attacks, according to McAfee Labs' Threats Report.

Unlike ransomware attacks, data breaches and cyber fraud tend to take longer for victims to discover. In Arceo's analysis, only about half of cyber incidents are discovered within a month of the actual incident date. This figure increases to 77% by six months and 94% by two years. The lesson for organizations, especially SMEs, is that they may experience incidents and associated losses, even if they've recently boosted their security controls and processes.

Once an organization discovers that a cyber event has occurred, local, state, federal, or international laws may require it to disclose the event and notify affected individuals. Notification laws exist in all 50 U.S. states, and the European Union's General Data Protection Regulation (GDPR) can apply broadly to any organization that holds personally identifiable data on EU citizens.

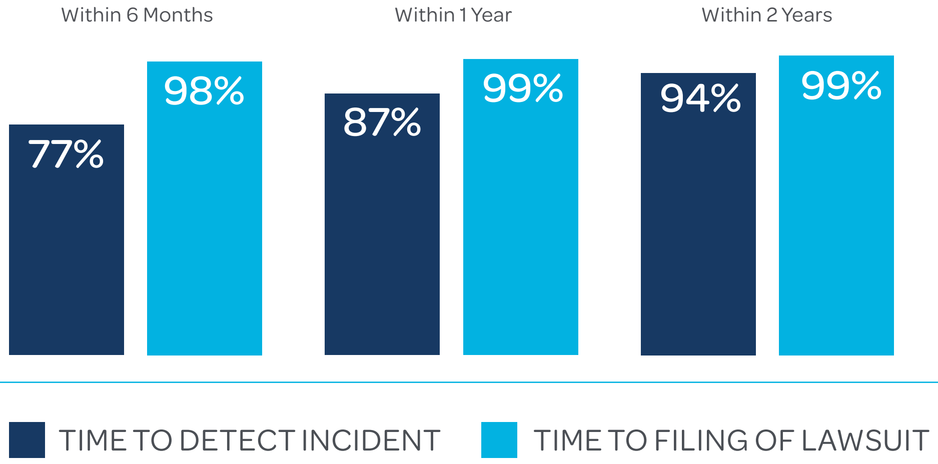
Disclosure of cyber events that involve a data breach often invites more bad news, in the form of lawsuits. Arceo's analysis of the Advisen data indicates that litigation generally follows breach disclosure within weeks, if indeed not days. Among those cyber incidents that eventually result in lawsuits, 96% of suits are filed within a month of the first public notice date. In addition, while there are time lags in the detection of cyber incidents that result in litigation in the Advisen Cyber Loss Data, litigation typically ensues quickly (see chart). Organizations therefore need to be prepared to respond to lawsuits quickly after incidents are discovered and announced.

$18M
IN COSTS
AFTER ATTACK
IN BALTIMORE

$17M
IN COSTS
AFTER ATTACK
IN ATLANTA

118%
INCREASE IN
RANSOMWARE
ATTACKS IN Q1 2019

CYBER INCIDENT DETECTION AND LITIGATION



Source: Advisen Ltd.

CONCLUSIONS

Arceo's findings that the impact of cyber risks on small to medium-sized enterprises is greater than on larger organizations, and the propensity of litigation following public disclosure of incidents such as data breaches, suggest that SMEs and the insurance industry should work together more. Small and midsize organizations clearly can take benefit from more resources to mitigate and respond to cyber risks, from understanding their exposures to improving cybersecurity, as well as defending litigation after disclosing an event. At the same time, insurers, agents, and brokers have an opportunity to provide enhanced cyber insurance products and risk management services to the small and midsize market segment.

Arceo's goal is to bridge two complex industries – cybersecurity and insurance – to combine and unlock the shared potential of these markets. To learn how Arceo is blending its expertise to create a single platform that delivers value to the insurance world and translates granular security information into quantifiable risks for insurers, brokers, and insureds, please contact us at contact@arceo.ai.

ABOUT ARCEO.AI

Arceo.ai is building a novel approach to securing enterprises from cyber threats by blending cyber security expertise, credible risk assessment, and risk transfer experience. Our end-to-end cyber risk analytics and insurance platform enables insurers and brokers to more accurately assess, underwrite, and manage cyber risks using curated security data for accuracy, AI for advanced risk assessment, and workflow automation for efficiency. Arceo is privately funded and headquartered in San Francisco, California, with offices in Baltimore and New York. For more information, visit www.arceo.ai

ABOUT ADVISEN LTD.

Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets and applications focus on large, specialty risks. Through Web Connectivity Ltd., Advisen provides messaging services, business consulting, and technical solutions to streamline and automate insurance transactions. Advisen connects a community of more than 200,000 professionals through daily newsletters, conferences, and webinars. The company was founded in 2000 and is headquartered in New York City, with offices in the U.S. and the U.K.

GLOSSARY

CYBER EXTORTION: A growing form of cyber crime that involves data encryption or the threat of disclosure of sensitive or embarrassing information. Perpetrators typically attempt to obtain payment in cryptocurrency, such as Bitcoin, to remain anonymous.

CYBER RISK: The risk of financial or physical loss, disruption of services, privacy violation, or damage to an organization's assets or reputation due to failure of the organization's information technology systems or a malicious act affecting such systems.

GENERAL DATA PROTECTION REGULATION (GDPR): Taking effect in May 2018, the GDPR applies to all individuals, companies, or organizations that process personal data on individuals residing in the European Union. It is one of the broadest and most restrictive data privacy regulations in the world. A similar regulation, the California Consumer Privacy Act, goes into effect for California residents in 2020.

PHISHING: A type of identity theft that uses email or fraudulent websites to collect information such as passwords, bank card data, and account information.

RANSOMWARE: Malicious software that encrypts data on an infected device. Perpetrators of ransomware attacks attempt to extort payment from the device's owner prior to delivering a software key to decrypt and recover the data.

SMALL TO MEDIUM-SIZED ENTERPRISE (SME): An organization with fewer than 1,000 employees.

SOCIAL ENGINEERING: A component of many types of cyber attacks that relies on human interaction, such as clicking a link to execute malware. Social engineering entices or deceives people into providing passwords or other sensitive information that facilitates an attack or other cyber crime.

SPEAR-PHISHING: A variant of phishing that uses personalized or specific information to gain access to personal or corporate data. Personalized communication or reference to a recent transaction, for example, are tools in spear-phishing attacks.

SPOOFING: A fraudulent or malicious attempt to obtain personal information or payment through communication by impersonating someone known to the recipient. Spoofing commonly uses email or telephone communication.