cysurance

White Paper #1

THE CYBER RISK MANAGEMENT TRIFECTA

December 2020

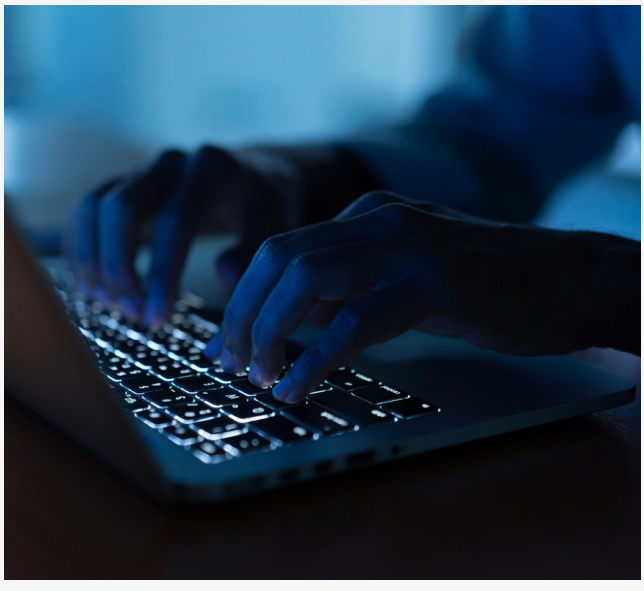
PRESENTED BY
Kirsten Bay

THE CYBER RISK MANAGEMENT TRIFECTA

Todays companies need to think about cyber risk holistically

The consequences of a data breach or cyberattack are too great to assume that cybersecurity technology will protect against any and all threats, especially when social engineering and human error remain such significant exposures. Business owners need to think about their corporate network like they do their home or car and build a complete strategy that protects, prepares and responds. Only with a cutting-edge cybersecurity infrastructure, comprehensive cyber governance and robust cyber insurance can this cyber risk management trifecta be achieved.

While homeowners and auto insurance are usually required by legislators or lenders, most would agree they are necessary to be truly prepared for the worst. Our homes are protected by security systems, fire alarms, cameras and smart devices and our cars feature collision detection systems, lane departure assist and automatic braking, yet we still worry about the worst happening. And even though there are building codes and traffic laws, we know accidents happen. So, while it is critical to build a strong firewall and encrypt data as well as regularly educate employees and update incident response plans, companies must also protect against “black swan” events – like COVID-19 – with robust cyber insurance.



THE CYBER RISK MANAGEMENT TRIFECTA

To date, companies have focused largely on building-out their security technology, with worldwide spending on cybersecurity expected to reach $133.7 billion by 2022. Research and advisory firm Gartner recommends enterprises should be spending 4-7% of their IT budgets on security, especially as companies need to comply with new privacy laws like the CCPA and SHIELD Act in New York, or GDPR in Europe. Companies are currently concentrating on proper authentication and authorization technologies, endpoint protection and security analytics and intelligence software. However, as the risk landscape expands, managed cybersecurity services are becoming more popular, representing the top segment of worldwide cybersecurity spending in 2019, at $64.2 billion. Gartner predicts such services will account for 50% of cybersecurity budgets by 2020.

In addition to security technology, many firms leverage cyber awareness training to manage their digital risks.

With 93% of cybersecurity professionals agreeing that humans and technology need to work together to detect and respond to cyber threats, one industry expert predicts this market will be worth $10 billion by 2027. And as the format transitions from once-a-year, mandatory classroom training sessions to continuous, interactive browser based training mixed with gamification and simulated phishing attacks, ROI's associated with cyber awareness training are improving. Security-related risks are reduced by 70% when a business invests in this area, and even the least effective training programs have a 7-fold return on investment, according to the Ponemon Institute.

THE CYBER RISK MANAGEMENT TRIFECTA

Yet despite the increased spending on cybersecurity technology and growing awareness, there is still work to be done. Last year there was a 424% increase in new small business cyber breaches, and the average cost of a data breach has increased 12% in the last five years. A fundamental conundrum also exists in that the threat actors are adapting, investing and learning too. Lone-wolf hackers are teaming up to create organized cybercrime syndicates, nation-states are engaging in cyberwarfare and threats have evolved from pranks and socially-inspired protests to orchestrated, highly-profitable attacks. While ransomware remains prevelant, with incident reports more than doubling in 2019, other risks are emerging as well, such as API abuse and application denial-of-service attacks.

Further, according to one survey, 30% of employees still don't know what phishing or malware is – making the 92.4% of malware delivered as an attachment in a malicious email a serious threat. In 2018, Verizon reported that 30% of phishing emails are opened and 12% are activated, meaning the links are clicked or the attachment is opened. Another study shows users clicking on mobile phishing links has increased 85% since 2011.

On average, an employee shares their password with 6 other coworkers, and half use the same password for personal accounts as for work accounts.

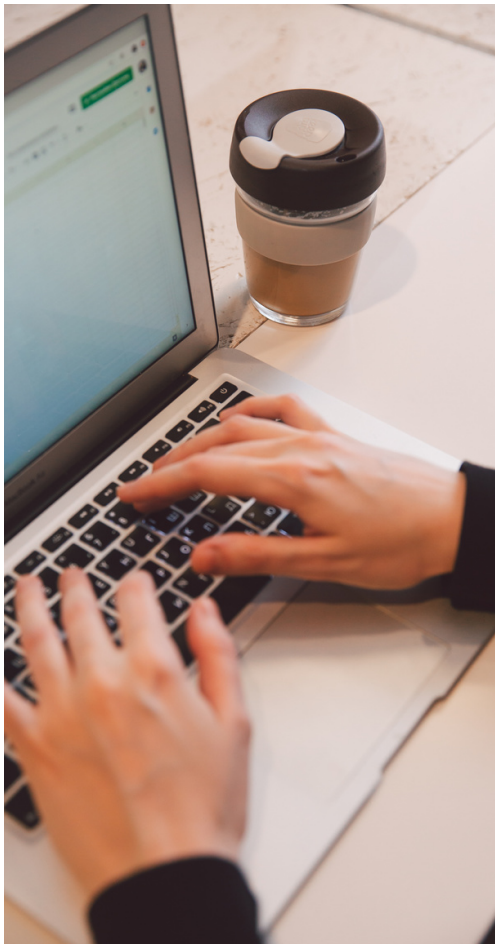
While cybersecurity and awareness are making strides, threat actors are also innovating and new attack vectors appearing overnight. And just like the lock on your front door can be picked or a driver might ignore a collision warning, even the best cybersecurity technology can be breached. Today, criminals are targeting cloud-based applications, leveraging swarm technology and 5G networks and using advanced malware that presents users with a replica web browser that records sensitive data.

THE CYBER RISK MANAGEMENT TRIFECTA

As society becomes more interconnected and additional industries and infrastructure move online, the risk is becoming more systemic. A Ponemon Institute/IBM study found breaches caused by a third party were the top factor in amplifying the cost of a breach, adding an average of $370,000 to the overall loss, but 93% of enterprises are expected to adopt IoT technology during 2020. In addition, 90% of cars will be connected to the internet and 3.5 billion cellular IoT connections will be installed. By 2025, more than 75 billion IoT devices will be connected to the web. Yet despite the increased spending on cybersecurity technology and growing awareness, there is still work to be done. A report from cybersecurity firm eSentire showed the real estate industry suffered the second most malware attacks in the second quarter of 2018, and last year there was a 424% increase in new small business cyber breaches.

The combination of these factors means companies simply cannot risk leaving their downside unprotected.

While cyber insurance direct written premiums grew 12% in 2019, the market totals just over $2.2 billion, and 91% of small businesses still don't have this critical protection. Further, many companies underestimate the long-term impact of a cyberattack, with the average cost to get a business back to normal after an attack ($955,429) outpacing the average cost of stolen assets ($879,582).



Even if you have the best cybersecurity software on the market and provide regular training to your employees, 52% of data breaches are the result of human error and system failure. The likelihood of unpredictable 'black swan' events like COVID-19 also remains. And since 86% of consumers won't or are unlikely to work with an organization that has suffered a data breach involving credit or debit card details, a cyber insurance claim payment may just help keep your company alive while you rebuild your business.

Kirsten Bay
CEO - Cysurance
kbay@cysurance.com

Cysurance is the next-generation cyber solution, protecting small businesses and their partners through affordable cyber insurance. Built on a proprietary platform, our program comes with a complete set of features to safeguard business continuity and insure against loss, protecting both revenue and recovery.

For more information, visit www.cysurance.com, follow us on LinkedIn, Facebook, Instagram and Twitter, or email us at info@cysurance.com.

cysurance