Are cyberattacks the next black swan event? - blueAPACHE

Canonical: https://www.blueapache.com/blog/are-cyberattacks-the-next-black-swan-event

Details:

We explore how organisations can prepare for cyber incidents with widespread consequences.

2017

A black swan event is an unexpected, high-profile event that is large in magnitude and consequence and is extremely difficult to predict. If cyberattacks are the next black swan event, is it possible for organisations to prepare themselves for it? The term black swan dates back to a period when it was widely believed that all swans are white. However, in 1697, after Dutch explorers first sighted black swans in Western Australia, the phrase came to indicate an occurrence that was previously thought to be inconceivable and has widespread ramifications. Black swan events are rationalised after the fact with the benefit of hindsight. Increasingly, cyberattacks are being classified as black swan events. The recent outbreak of WannaCry ransomware and other such occurances reinforce that cyber threats that were once considered impossible are now occurring on a daily basis and the ramifications are not limited to just one organistaion, industry or country. Cyberattacks have resulted in billions of dollars being lost to ransomware payoffs , shutting down of systems forcing companies offline and mass leaking of confidential customer data leading to loss of reputation and customer trust. Australian Securities and Investment Commission (ASIC) chairman Greg Medcraft recently warned businesses that a significant cyberattack could be the next black swan event. Medcraft attributed the increasing number, and impact, of attacks to a lack of transparency and reporting of such attacks. ASIC has been urging companies to review their exposure to cyberattacks and to step up their plans for more cyber security. Cyber resilience gains even more importance when organisations are faced with stricter laws governing data breaches and privacy and higher community expectations. Can SMEs prepare themselves for the next event? For many small and medium-sized enterprises (SMEs), a cyberattack is not a black swan event, but an inevitability. From malware to DDoS attacks, from phishing campaigns to ransomware, today’s threat landscape is expanding continuously. It is no longer a viable strategy for organisations to just respond to security breaches, rather the emphasis is on preventing them. This requires a proactive approach to security that covers everything from firewalls to end point security, where staff are informed and aware of potential threats and there are regular backups of all critical systems and data. For many SMEs this is a big ask. This is where the ‘as a service’ model can bring the benefits of industry leading experts and technologies within easy reach of SMEs in an affordable, scalable and predictable offering. Security as a Service (SECaaS) is a growing industry that is set to be worth $US8.52b by 2020. This model eases the financial and resource constraints faced by SMEs and transfers accountability to a single trusted SECaaS provider. For more information on SECaaS (or to validate your existing security strategy), contact the our security team .

What is a black swan event, as described in the blueAPACHE article?

A black swan event is an unexpected, high-profile event that is large in magnitude and consequence and is extremely difficult to predict. The term dates back to when it was believed all swans were white, until Dutch explorers first sighted black swans in Western Australia in 1697, after which the phrase came to mean an occurrence previously thought inconceivable but with widespread ramifications. Black swan events are rationalised after the fact with the benefit of hindsight.

Why are cyberattacks increasingly being classified as black swan events?

cyber threats once considered impossible are now occurring on a daily basis, and their ramifications are not limited to a single organisation, industry, or country. The outbreak of WannaCry ransomware and similar occurrences are cited as reinforcing this classification, with cyberattacks resulting in billions of dollars lost to ransomware payoffs, systems being shut down forcing companies offline, and mass leaking of confidential customer data leading to loss of reputation and customer trust.

Who warned that a significant cyberattack could be the next black swan event, and why?

Australian Securities and Investment Commission (ASIC) chairman Greg Medcraft warned businesses that a significant cyberattack could be the next black swan event. He attributed the increasing number and impact of attacks to a lack of transparency and reporting of such attacks, and ASIC has been urging companies to review their exposure to cyberattacks and step up their cyber security plans.

Why does cyber resilience matter even more for organisations today, ?

Cyber resilience gains even more importance when organisations are faced with stricter laws governing data breaches and privacy, along with higher community expectations.

Is a cyberattack really a 'black swan' event for small and medium-sized enterprises (SMEs)?

for many SMEs, a cyberattack is not a black swan event but an inevitability. Today's threat landscape—including malware, DDoS attacks, phishing campaigns, and ransomware—is continuously expanding.

What is Security as a Service (SECaaS) and how can it help SMEs, ?

Security as a Service (SECaaS) is a growing industry that was set to be worth US$8.52 billion by 2020. The 'as a service' model brings the benefits of industry-leading experts and technologies within easy reach of SMEs in an affordable, scalable, and predictable offering, easing the financial and resource constraints faced by SMEs and transferring accountability to a single trusted SECaaS provider.

How can a business get more information about SECaaS or validate its security strategy ?

We advise contacting our security team via the site's contact page for more information on SECaaS or to validate an existing security strategy.